INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD)
© 2026 IJNRD | Volume 11, Issue 10, October 2026 | ISSN: 2456-4184 | IJNRD.ORG

Perspectives on Cybercrime and Digital Vulnerability among Rural Youth in Himachal Pradesh:

An Empirical Assessment of Emerging Challenges in the Digital Society

[1]Dr. Sanjeev Kumar [2]Shubham Bhardwaj [3]Pragati Sharma

[1] Sr. Research Officer, Department of Interdisciplinary Studies, Himachal Pradesh University, Shimla.
[2] Student, MBA-RD, Department of Interdisciplinary Studies, Himachal Pradesh University, Shimla.
[3] Research Scholar, Department of Interdisciplinary Studies, Himachal Pradesh University, Shimla.

Abstract: The widespread adoption of digital connectivity and social media platforms has transformed the lives of youth in rural India, providing new opportunities while also introducing significant vulnerabilities or risks like cybercrime and digital exploitation. This infrastructural success, however, has not been met with adequate efforts to ensure the safe and responsible use of these technologies. This paper aims to assess the vulnerabilities and issues related to cybercrime and social media that rural youth face. The study explores the relationship between their digital access, awareness levels, and the risks or vulnerabilities they encounter online. The research also highlights a general acknowledgment of the rise of several scams and the risk of unintentional data sharing among rural youth. These results reflect the urgent need for targeted, context-specific digital literacy interventions.

Index Terms- Digital Literacy, Social media, Rural youth, Digital Divide

1. INTRODUCTION

The rapid expansion of digital connectivity has transformed the social, cultural, and economic lives of youth across the globe. Social media platforms such as Facebook, Instagram, WhatsApp, and YouTube have become central to communication, networking, entertainment, and learning. These platforms function not only as channels of interpersonal interaction but also as gateways to educational resources, employment opportunities, and civic engagement. For rural youth, in particular, social media bridges geographical divides by enabling participation in networks and conversations that were previously inaccessible. However, the same digital avenues that promote empowerment also introduce significant risks, particularly in the form of cybercrime and digital exploitation (Livingstone & Smith, 2014). The increasing dependence on online spaces for education, employment opportunities, and social interaction has heightened the exposure of rural youth to threats such as misinformation, identity theft, financial fraud, and online harassment. These risks are particularly concerning in contexts where digital literacy is limited, and awareness of safe online practices remains underdeveloped.

The digital revolution in India, accelerated by the proliferation of low-cost smartphones and affordable internet access, has significantly expanded connectivity in rural areas. Mobile data packages and affordable handsets have made it possible for even economically disadvantaged families to maintain internet-enabled devices, thereby increasing rural participation in the digital economy. In addition, government initiatives under programs such as *Digital India* and *BharatNet* have promoted inclusivity by expanding digital infrastructure to villages and underserved regions. These efforts signify important progress in closing the digital divide between rural and urban population. Nevertheless, this infrastructural success has not been matched by adequate efforts to ensure the safe and responsible use of digital technologies. Scholars argue that access without awareness increases vulnerability, creating a digital environment where rural youth may easily become targets of manipulation, exploitation, and cyber victimization (Mihailidis & Thevenin, 2013).

Cybercrime in the context of rural youth is multidimensional, encompassing both technical risks and psychological implications. Unlike urban youth, who may have greater access to formal training and awareness campaigns, rural youth are often left to navigate online spaces with limited guidance. This lack of preparedness creates fertile ground for digital exploitation. Exposure to misleading information, fake job offers, and fraudulent schemes often exploits the aspirations of rural youth, who increasingly rely on digital platforms for guidance and opportunities (Guess, Nyhan, & Reifler, 2020). False advertisements and misleading posts are particularly effective because they play upon the genuine needs of young people in rural areas, many of whom are seeking better education, employment, or financial stability. Furthermore, cyberbullying, online harassment, and peer pressure manifest in subtle yet damaging ways, contributing to mental health challenges, low self-esteem, and social isolation (Wolak, Mitchell, & Finkelhor, 2006). These problems are exacerbated in rural contexts where counselling resources, peer support groups, or helplines are either absent or difficult to access. Such experiences are often underreported in rural settings due to stigma, lack of institutional support, and limited knowledge about legal redress mechanisms (Livingstone & Smith, 2014).

Another dimension of vulnerability arises from romance scams, blackmail, and emotional exploitation, which exploit the limited awareness and trust of rural internet users. Romance scams, for example, typically involve perpetrators establishing emotional connections with victims, only to manipulate them for money or personal information. This type of exploitation has profound emotional as well as financial consequences, particularly for rural youth who may lack prior exposure to the warning signs of such fraudulent activity. Similarly, blackmail and online threats contribute to psychological distress, often leaving victims feeling isolated and powerless. Scholars note that such forms of manipulation not only result in financial and psychological harm but also highlight the inadequacies of digital literacy frameworks in rural contexts. Without systematic education on recognizing these risks, rural youth remain particularly susceptible.

The lack of structured awareness programs in schools and community institutions further aggravates the issue. Although there is growing recognition of the importance of cyber safety education, formal mechanisms to teach young people about secure online practices are scarce in rural India. Even when youth recognize the importance of cyber safety education, their willingness to participate in awareness initiatives may be low due to cultural factors, irrelevance of content, or limited engagement strategies (Mihailidis & Thevenin, 2013). For example, workshops or sessions designed in urban contexts may not adequately reflect the realities of rural youth, whose online behaviors, priorities, and vulnerabilities may differ. This mismatch highlights the importance of culturally relevant and context-specific approaches that directly address the lived experiences of rural populations.

The research paper, therefore, focuses on the assessment of cybercrime vulnerabilities prevalent among rural youth. It explores the interplay between digital access, awareness levels, and the risks encountered in online environments. By situating these challenges within broader discussions of digital literacy, social protection, and youth development, this paper highlights the urgent need for multi-stakeholder interventions. Schools, non-governmental organizations (NGOs), government programs, and community networks all have a role to play in fostering safer digital ecosystems. More importantly, context-specific strategies are essential, as the vulnerabilities of rural youth differ significantly from those of their urban counterparts due to socio-economic disparities, cultural contexts, and infrastructural limitations.

The survey was conducted among rural youth of *Jhandutta* Gram Panchayat of Himachal Pradesh which highlights significant gaps in digital safety among rural youth. The figures demonstrate the everyday challenges rural youth face in identifying trustworthy sources of online content. Although most respondents denied experiencing cyberbullying, around one-fourth admitted exposure to harassment or peer pressure, reflecting the psychological costs of digital participation. Notably, 70% observed rising romance scams, and nearly 28% faced threats or blackmail online, underscoring the prevalence of emotional manipulation in cyberspace. On a positive note, many participants reported practicing basic safety measures such as maintaining strong passwords, which indicates a foundational level of awareness. Several technical nudges like password meters or basic digital literacy regarding account security can function as the first line of defence against hacking and identity theft (Ur et al. 2012). However, only 46.6% showed willingness to attend awareness programs, reflecting the gap between acknowledging risks and actively engaging in preventive action. Collectively, these patterns reveal the paradox of increasing awareness but limited participation in capacity-building initiatives, reinforcing the urgent need for tailored and accessible digital literacy interventions in rural areas.

2. STATEMENT OF THE PROBLEM

The rapid expansion of digital infrastructure and affordable smartphones in India has successfully integrated rural youth into the global digital economy, bridging the historical digital access divide. However, this infrastructural success has inadvertently created a new, critical vulnerability that is a significant gap between digital connectivity and digital literacy. Rural youth in regions like Himachal Pradesh are increasingly relying on social media platforms for education and employment, yet they navigate these spaces without adequate guidance or awareness of safe online practices. Consequently, they face disproportionate exposure to online threats, including educational misinformation, fake job offers, romance scams, and cyberbullying. The problem is exacerbated by the absence of context-specific, culturally relevant digital safety programs in rural schools and communities, leaving youth susceptible to financial and psychological exploitation. Furthermore, social stigma and a lack of institutional support result in a significant hesitation to report cybercrimes, with many victims remaining silent. Therefore, the core problem addressed in this study is the urgent need to assess the specific cybercrime vulnerabilities of rural youth and bridge the gap between digital access and comprehensive, tailored digital literacy interventions.

3. RESEARCH METHODOLOGY

This empirical study utilized a quantitative research design to assess the digital vulnerabilities of rural youth. Primary data was collected through a structured survey conducted among the youth of the Jhandutta Gram Panchayat in Himachal Pradesh. Primary data was collected from a sample of 120 respondents using a structured, self-administered questionnaire designed to assess demographic variables, digital competencies, online behaviours, and knowledge of cyber threats. The survey instrument employed a five-point Likert scale, ranging from "Strongly Agree" to "Strongly Disagree," to measure various dimensions of digital exposure and behaviour. Key parameters assessed included experiences of online harassment, exposure to employment scams, encounters with misinformation, digital blackmail, and hesitation in reporting online issues.

4. ASSESSMENT OF ONLINE VULNERABILITIES AND CHALLENGES

4.1 Experience of Online Harassment

Experience of online harassment refers to an individual's personal encounter with bullying, threats, or abusive behaviour on digital platforms. This experience provides insight into the prevalence, severity, and emotional consequences of cyberbullying within a community. Understanding such experiences is essential for assessing the psychological and social impact of online harassment, identifying vulnerable groups, and designing effective prevention and support strategies. Studies suggest that exposure to online harassment can significantly affect mental health and well-being (Patchin & Hinduja, 2014).

TABLE-1
Exposure to Online Bullying and Harassment

Response category	Frequency	Percent	Valid percent
Strongly Agree	15	12.5%	12.5%
Agree	16	13.3%	13.3%
Neutral	9	7.5%	7.5%
Disagree	76	63.3%	63.3%
Strongly Disagree	4	3.3%	3.3%
Total	**120**	**100.0%**	**100.0%**

Source: Primary Data

The majority of respondents (63.3% disagreed and 3.3% strongly disagreed) reported they have not experienced online bullying. However, 12.5% strongly agreed and 13.3% agreed that they had faced such issues, with 7.5% neutral. This suggests that although a smaller group has faced harassment, the experience is still significant and should not be overlooked. With the increase accessibility of internet comes several vulnerabilities as well. These findings justify the inclusion of online safety and reporting procedures in social media literacy campaigns.

4.2 Hesitation in Reporting Online Issues

Hesitation in reporting online issues refers to the reluctance of individuals to report cyber incidents due to fear, social stigma, or peer pressure. Such hesitation can prevent timely action against cybercrime and allows harmful behaviour to persist. Understanding these emotional and cultural barriers is crucial for designing effective awareness programs and encouraging responsible digital behaviour (Livingstone et al., 2011).

TABLE-2
Hesitation in Reporting Online Issues Due to Fear or Social Pressure

Response category	Frequency	Percent	Valid percent
Strongly Agree	15	12.5%	12.5%
Agree	14	11.7%	11.7%
Neutral	12	10.0%	10.0%
Disagree	73	60.8%	60.8%
Strongly Disagree	6	5.0%	5.0%
Total	**120**	**100.0%**	**100.0%**

Source: Primary Data

A majority (60.8%) of respondents disagreed with the statement, suggesting they are open to discussing online problems. However, 12.5% strongly agreed and 11.7% agreed that fear or pressure affected their willingness to speak up. Neutral responses stood at 10%. These findings indicate that while many feel comfortable addressing issues, a notable number remain silent due to stigma or hesitation. Awareness programs must include peer support and safe reporting channels to break this silence.

4.3 Exposure to Online Scams

Exposure to online scams refers to instances where individuals encounter fraudulent messages, fake job offers, phishing links, or deceptive content on digital platforms. Such exposure highlights the increasing prevalence of cyber fraud and the risks posed to unsuspecting users. Understanding this exposure is critical for developing digital literacy skills and preventive strategies to mitigate online financial and personal harm (Button et al., 2017).

TABLE-3
Exposure to Fake Job Offers and Suspicious Messages on Social Media

Response category	Frequency	Percent	Valid percent
Strongly Agree	7	5.8%	5.8%

Agree	29	24.2%	24.2%
Neutral	7	5.8%	5.8%
Disagree	72	60.0%	60.0%
Strongly Disagree	5	4.2%	4.2%
Total	**120**	**100.0%**	**100.0%**

Source: Primary Data

A large portion of respondents (60%) disagreed, and 4.2% strongly disagreed, indicating that most have not encountered fake job offers or suspicious messages. However, 24.2% agreed and 5.8% strongly agreed, with 5.8% neutral. This shows that while such experiences are not widespread, a significant minority has encountered fraudulent job-related communication. Due to increase levels of unemployment among youth, the issue becomes more critical. These findings emphasize the need to educate youth on how to recognize and avoid employment scams, particularly in rural or less-informed areas.

4.4 Exposure to Online Hate Speech

Exposure to online hate speech refers to situations where individuals witness or personally encounter abusive, offensive, or discriminatory language on social media and other digital platforms. This exposure reflects the widespread presence of harmful content online and underscores the importance of digital literacy, moderation tools, and awareness to protect users and promote respectful online interactions (Gagliardone et al., 2015). Emphasizing digital consent is essential for fostering ethical interactions and protecting the rights of all users in increasingly connected online spaces (Livingstone et al., 2018).

TABLE-4
Exposure to and Victimization by Online Hate Speech

Response Category	Frequency	Percent	Valid Percent
Strongly Agree	5	4.2%	4.2%
Agree	31	25.8%	25.8%
Neutral	6	5.0%	5.0%
Disagree	76	63.3%	63.3%
Strongly Disagree	2	1.7%	1.7%
Total	**120**	**100.0%**	**100.0%**

Source: Primary Data

Most respondents (63.3%) disagreed and 1.7% strongly disagreed with having experienced or witnessed hate speech. Meanwhile, 25.8% agreed and 4.2% strongly agreed, and 5% were neutral. Although a majority have not encountered such incidents, a notable portion still has. This reflects the presence of toxic online behaviour, which may go unreported or unnoticed. Awareness campaigns should encourage victims to speak up and report such offenses, and social platforms must monitor hate content more actively.

4.5 Encounter with Mis-information

Encounter with misinformation refers to individuals coming across false news, propaganda, or misleading content on social media platforms. This highlights the critical need for media literacy and fact-checking skills, enabling users to verify information before believing or sharing it, thereby reducing the spread of misinformation and promoting responsible digital behaviour (Lewandowsky, Ecker, & Cook, 2017). Account security awareness is also very important as an individual's knowledge and practices will help in protecting social media accounts from unauthorized access. This includes using strong passwords, enabling two-factor authentication, and identifying suspicious activities to prevent hacking and cyber threats (Florêncio & Herley, 2007).

TABLE-5
Exposure to False News and Propaganda

Response Category	Frequency	Percent	Valid Percent
Strongly Agree	31	25.8%	25.8%
Agree	42	35.0%	35.0%
Neutral	9	7.5%	7.5%
Disagree	37	30.8%	30.8%
Strongly Disagree	1	0.8%	0.8%
Total	**120**	**100.0%**	**100.0%**

Source: Primary Data

A substantial majority acknowledged encountering fake news, with 35% agreeing and 25.8% strongly agreeing. Still, 30.8% disagreed, and 0.8% strongly disagreed, while 7.5% were neutral. These results highlight that false information is a common experience for youth online. It emphasizes the urgent need for fact-checking education, critical thinking, and training in identifying credible sources to combat digital misinformation and propaganda.

4.6 Experience of Online Threats

Experience of online threats refers to instances where individuals encounter threatening messages, blackmail, or intimidation via digital platforms. Such experiences highlight the prevalence of cybercrime and the critical need for awareness, timely reporting, and protective measures to ensure online safety (Patchin & Hinduja, 2010). Emphasizing digital consent is essential for fostering ethical interactions and protecting the rights of all users in increasingly connected online spaces (Livingstone et al., 2019).

TABLE-6

Exposure to Online Threats and Blackmail

Response category	Frequency	Percent	Valid percent
Strongly Agree	15	12.5%	12.5%
Agree	19	15.8%	15.8%
Neutral	5	4.2%	4.2%
Disagree	78	65.0%	65.0%
Strongly Disagree	3	2.5%	2.5%
Total	**120**	**100.0%**	**100.0%**

Source: Primary Data

Most respondents (65%) disagreed and 2.5% strongly disagreed, showing they haven't experienced online threats. Yet, 15.8% agreed and 12.5% strongly agreed, indicating that a meaningful number have faced digital blackmail or intimidation. With the coming of digital revolution came several technological innovations such as AI which has proved to be both useful and harmful in its use. These numbers stress the importance of building safe reporting systems, supporting victims, and informing users about legal protections and how to document such incidents for evidence.

4.7 Educational Misinformation Online

Educational misinformation online refers to the dissemination of false or misleading information regarding exams, results, admissions, or job opportunities. This can cause confusion, stress, and misinformed decisions among students and job seekers, emphasizing the importance of verifying information through credible sources (Vraga & Bode, 2020). This limited awareness can be eradicated by addressing the gap through targeted education, awareness campaigns, and social media literacy programs is essential to enhance safe online practices and protect rural youth from cyber threats (Kshetri, 2014)

TABLE-7

Exposure to Fake News Regarding Exams and Employment

Response category	Frequency	Percent	Valid percent
Strongly Agree	15	12.5%	12.5%
Agree	19	15.8%	15.8%
Neutral	5	4.2%	4.2%
Disagree	78	65.0%	65.0%
Strongly Disagree	3	2.5%	2.5%
Total	**120**	**100.0%**	**100.0%**

Source: Primary Data

Most respondents (65%) disagreed and 2.5% strongly disagreed that they have encountered fake educational news. Only 12.5% strongly agreed and 15.8% agreed, with 4.2% neutral. While the majority may not perceive a high volume of educational misinformation, the experiences of the minority indicate that such content still circulates. Awareness must be raised, especially in exam season or job recruitment phases, to prevent panic or exploitation due to misleading posts .

4.8 Unintentional Data Sharing

Unintentional data sharing refers to instances where youth unknowingly disclose personal or sensitive information on social media platforms, which can subsequently be misused by cybercriminals or third parties. Such inadvertent sharing highlights the critical

need for digital awareness, cautious online behaviour, and education on privacy settings to protect personal data and reduce vulnerability to cyber threats (Livingstone & Haddon, 2009).

TABLE-8
Perceptions on Unintentional Data Sharing and Online Misuse

Response category	Frequency	Percent	Valid percent
Strongly Agree	28	23.3%	23.3%
Agree	58	48.3%	48.3%
Neutral	6	5.0%	5.0%
Disagree	27	22.5%	22.5%
Strongly Disagree	1	0.8%	0.8%
Total	**120**	**100.0%**	**100.0%**

Source: Primary Data

Most respondents agree with this concern as 48.3% agreed and 23.3% strongly agreed. Around 22.5% disagreed and 5% were neutral. This response confirms that users are aware of the unintentional risks associated with oversharing. It also highlights the need to reinforce privacy education, especially around what not to share publicly like OTPs, addresses, and official documents which can be exploited for identity theft or scams.

5. CONCLUSIONS

The research presented in this paper provides a critical examination of the online risks and vulnerabilities faced by rural youth of Himachal Pradesh, a demographic at the forefront of the country's digital revolution. The rapid expansion of digital infrastructure and affordable technology has successfully fostered greater digital inclusion by bridging geographical divides and connecting rural populations to a global information network. However, this success has created a new, more subtle form of the "digital divide" one not based on access, but on the profound gap between the ease of connectivity and the lack of essential digital literacy needed to navigate the online world safely. Social media platforms, while offering avenues for social, educational, and economic empowerment, simultaneously act as conduits for a wide array of threats, including cybercrime, misinformation, and online harassment.

The data analysis from this study reveals a complex picture of digital engagement and awareness. On one hand, there is a clear acknowledgment among the youth that online threats are real. A significant majority of respondents reported encountering misinformation or false news, and more than half of them have been exposed to fake information related to critical opportunities like jobs or education. These numbers indicate that the problem is not a lack of exposure to threats, but rather an issue of how to effectively respond to them.

On the other hand, the issue is further compounded by the finding that nearly a quarter of the youth have experienced online bullying or harassment, underscoring that these are not abstract risks but concrete realities for many. The data also showed a significant reluctance to participate in proactive safety education programs, despite acknowledging its importance. This suggests that existing educational models may not be appealing or relevant to this demographic, creating a major barrier to effective intervention.

The central aim of this study was to move beyond the simple metrics of internet access and to understand the lived experiences and actual vulnerabilities of rural youth. It sought to understand their awareness of online risks, their confidence in handling these threats, and their willingness to engage in protective behaviors. By surveying a diverse group of young people, the paper provides an empirical foundation for understanding the real-world implications of the digital revolution. The findings suggest that while these youth are active participants in online spaces, they often lack the foundational knowledge and practical skills required for effective self-protection. This vulnerability is not merely a theoretical concern; it has tangible consequences, affecting their security, financial well-being, and psychological health.

The most critical takeaway from this research is that simply providing internet access is an incomplete solution. The assumption that users will naturally develop the necessary skills to protect themselves is flawed and leaves a vulnerable population exposed to significant harm. The study provides concrete evidence that a substantial portion of rural youth are navigating a dangerous digital landscape without a reliable map. The data-driven findings on misinformation, scams, underscore the urgent need for a shift in strategy. It is not enough to simply build the roads; we must also teach people how to drive on them safely.

Digital literacy programs must be redesigned to be more engaging, practical, and targeted. This means moving beyond passive awareness campaigns and implementing hands-on training that teaches youth how to identify and report scams, how to manage their digital footprint, and how to use critical thinking to evaluate online content. Educational efforts must also be tailored to the specific context of rural life, addressing unique vulnerabilities such as scams related to agricultural schemes, employment opportunities, and

government initiatives. Furthermore, a collaborative approach is essential, involving government bodies, schools, local community leaders, and NGOs to create a cohesive and accessible support system. By ensuring that formal reporting mechanisms, like the Cyber Cell, are well-publicized and user-friendly, we can empower youth to take effective action when they encounter threats. The future of a truly inclusive and equitable digital India depends on our ability to prioritize not just connectivity, but also the safety, security, and well-being of its youngest and most promising citizens.

References

(1) Livingstone, S., & Smith, P. K. (2014). Annual research review: Harms experienced by child users of online and mobile technologies: The nature, prevalence, and management of sexual and aggressive risks in the digital age. *Journal of Child Psychology and Psychiatry, 55*(6), 635–654. https://doi.org/10.1111/jcpp.12197
(2) Mihailidis, P., & Thevenin, B. (2013). Media literacy as a core competency for engaged citizenship in participatory democracy. *American Behavioral Scientist, 57*(11), 1611–1622. https://doi.org/10.1177/0002764213489015
(3) Guess, A., Nyhan, B., & Reifler, J. (2020). Exposure to untrustworthy websites in the 2016 US election. *Nature Human Behaviour*, 4(5), 472–480. https://doi.org/10.1038/s41562-020-0833-x
(4) Wolak, J., Mitchell, K. J., & Finkelhor, D. (2006). Online victimization of youth: Five years later. *National Center for Missing & Exploited Children*. Retrieved from https://www.unh.edu/ccrc/pdf/CV138.pdf
(5) Patchin, J. W., & Hinduja, S. (2014). *Cyberbullying: Identification, prevention, and response*. Cyberbullying Research Center.
(6) Abawajy, J. H. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology, 33*(3), 237–248.
(7) Livingstone, S., Haddon, L., Görzig, A., & Ólafsson, K. (2011). *Risks and safety on the internet: The perspective of European children*. EU Kids Online.
(8) Button, M., & Cross, C. (2017). *Cyber frauds, scams and their victims*. Routledge. https://doi.org/10.4324/9781315628585
(9) Gagliardone, I., Gal, D., Alves, T., & Martinez, G. (2015). *Countering online hate speech*. UNESCO Publishing.
(10) Lewandowsky, S., Ecker, U. K. H., & Cook, J. (2017). Beyond misinformation: Understanding and coping with the "post-truth" era. *Journal of Applied Research in Memory and Cognition, 6*(4), 353–369. https://doi.org/10.1016/j.jarmac.2017.07.008
(11) Patchin, J. W., & Hinduja, S. (2010). Cyberbullying and self-esteem. *Journal of School Health, 80*(12), 614–621. https://doi.org/10.1111/j.1746-1561.2010.00548.x
(12) Vraga, E. K., & Bode, L. (2020). Defining misinformation and understanding its correction in health and science contexts. *Proceedings of the National Academy of Sciences, 117*(27), 15596–15601. https://doi.org/10.1073/pnas.1912444117
(13) Florêncio, D., & Herley, C. (2007). A large-scale study of web password habits. *Proceedings of the 16th International Conference on World Wide Web*, 657–666. https://doi.org/10.1145/1242572.1242657
(14) Ur, B., Kelley, P. G., Komanduri, S., Lee, J., Maass, M., Mazurek, M. L., Passaro, T., Stephens, R., Tian, L., & Cranor, L. F. (2012). How does your password measure up? The effect of strength meters on password creation. In *Proceedings of the 21st USENIX Security Symposium* (pp. 65–80).
(15) Livingstone, S., Stoilova, M., & Nandagiri, R. (2019). *Children's data and privacy online: Growing up in a digital age. An evidence review*. London School of Economics and Political Science (LSE).
(16) Livingstone, S., & Haddon, L. (2009). *Kids online: Opportunities and risks*. Bristol, UK: Policy Press.
(17) Kshetri, N. (2014). The emerging role of Big Data in key development issues: Opportunities, challenges and concerns. *Big Data & Society*, 1(2). https://doi.org/10.1177/2053951714564227

Copyright & License:
© Authors retain the copyright of this article. This work is published under the Creative Commons Attribution 4.0 International License (CC BY 4.0), permitting unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.