

Impact of Socio-Economic Factors on Digital Literacy and Security

Jozef Lukáč¹, Zuzana Kudlová¹, Janka Kopčáková¹, Peter Gallo²

¹ Department of Corporate Financial Management, Faculty of Business Economy with seat in Košice, University of Economics in Bratislava, Tajovského 13, 04001 Košice, Slovak Republic

² Faculty of Arts Institute of Educology and Social Work, University of Presov, Ul. 17. novembra č. 1080 78 Prešov, Slovak Republic

Abstract – In the current digital environment, where misinformation and cyber threats pose significant challenges, developing and implementing effective strategies to enhance digital literacy and security is essential. This study examines Slovakia's approaches to individual digital management, with a focus on policies and initiatives aimed at increasing digital literacy and strengthening cybersecurity. A comprehensive analysis of demographic and socio-economic factors, including HDI, education levels, internet access rates, and others, is utilized to identify patterns that may influence the effectiveness of these policies. Methodologies such as regression analyses and clustering are employed to identify key factors impacting citizens' digital literacy and their ability to respond effectively to cyber threats. The findings indicate that a high HDI and availability of educational resources are associated with an enhanced capacity for citizens to critically analyze and safely engage with online content. Based on the analysis, targeted educational programs are recommended to address the specific needs of different demographic groups and raise awareness of cybersecurity.

Based on the analysis, targeted educational programs are recommended to address the specific needs of different demographic groups and raise awareness of cybersecurity. This approach has the potential to not only enhance individual protection against digital threats but also to strengthen overall digital literacy in society.

Keywords – Digital literacy, cybersecurity, individual digital management, misinformation, socio-economic factors.

1. Introduction

In the current digital era, the ability of individuals to effectively use information and communication technologies is crucial for their daily lives and work. Digital literacy and security are critical aspects that influence how individuals interact with digital content, protect their personal data, and recognize false information. In the context of an ever-changing digital environment, it is important to understand how various demographic and socio-economic factors affect these abilities. This study focuses on analyzing the relationships between the Human Development Index (HDI), education levels, internet access, and digital literacy in different countries. Revised cluster analysis and regression models were utilized to examine how these factors influence individuals' ability to correctly identify and respond to misinformation and cyber threats. The main aim of this study is to provide a deeper understanding of the dynamics of digital literacy and security and to propose effective educational policies and strategies to enhance digital resilience.

The basis of the analysis is the hypothesis that countries with higher HDI, better education systems, and broader internet access will have higher levels of digital literacy and better abilities among citizens to recognize and verify information. It is also hypothesized that security incidents and data loss are significant factors contributing to the failure to verify information, while redirection to fake websites significantly increases the risk of identity theft.

DOI: 10.18421/TEM141-81

<https://doi.org/10.18421/TEM141-81>

Corresponding author: Jozef Lukáč,
Department of Corporate Financial Management, Faculty of Business Economy with seat in Košice, University of Economics in Bratislava, Tajovského 13, 04001 Košice, Slovak Republic


Email: jozef.lukac@euba.sk

Received: 30 May 2024.

Revised: 28 October 2024.

Accepted: 18 November 2024.

Published: 27 February 2025.

 © 2024 Jozef Lukáč, Zuzana Kudlová, Janka Kopčáková & Peter Gallo; published by UIKTEN. This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 4.0 License.

The article is published with Open Access at <https://www.temjournal.com/>

2. Theoretical Framework

The significance of education for digital literacy is well documented in the literature. Studies show that higher levels of education lead to better abilities to analyze and manage digital content [1]. Educational programs that integrate digital skills into the curriculum can significantly improve digital literacy [2]. According to Karpati, digital skills acquired in the school environment have a long-term positive impact on individuals' ability to critically evaluate online content. Internet access is another key factor influencing digital literacy [3]. Other researchers found that the availability and quality of internet connections are crucial for the development of digital skills [4]. Similar conclusions are drawn by Arafah, B., & Hasyim, M. [5], who identified a strong correlation between internet access and digital literacy. In Slovakia, internet access is gradually improving, which positively affects the digital capabilities of the population [6].

Studies demonstrate that economic conditions, including income and employment, influence digital literacy. Hargittai and Helsper emphasize that economic stability allows individuals to invest in technology and education, which subsequently increases their digital literacy [7], [8]. According to Nurdiani, T. W et al [9], higher income correlates with better accessibility and use of digital resources. Countries with a high human development index (HDI) tend to show better results in cybersecurity [10]. Research has found that higher levels of education and income allow greater access to security resources and technologies, which enhances protection against cyber threats [11]. In Slovakia, a high HDI is associated with higher levels of awareness and preparedness for cyber threats [12].

Targeted educational programs can significantly contribute to increasing awareness and the ability of individuals to respond to digital threats. Research by Tondeur and Ertmer indicates that educational programs incorporating cybersecurity have a positive impact on the preparedness of students and citizens to face digital threats [13], [14]. Various initiatives supporting digital literacy and security are being implemented in Slovakia, as confirmed by recent research and government reports [15].

Cybersecurity and digital literacy are also influenced by cultural and regional differences. Hofstede's research shows that cultural values affect how individuals approach technology and security [16]. According to Urbancikova, N. et al [17], and Viliňová, K., et al [18], there are regional differences in the approach to digital skills and security, which are also evident in Slovakia.

3. Methodology

The primary aim of this research is to analyze and identify the impact of demographic and socio-economic factors on the digital literacy and cybersecurity of citizens in OECD countries. The research seeks to determine how various factors including education, internet access, and socio-economic development measured by HDI, influence individuals' ability to correctly identify and respond to false information and online threats. Additionally, this study focuses on formulating recommendations for policymakers and educational authorities that could lead to more effective strategies to improve digital literacy and security in the country.

The research is based on data analysis obtained from publicly available sources and databases from 2022, including information on digital literacy, cybersecurity, and socio-economic and demographic factors. Data were extracted from international databases such as the World Bank and the Organisation for Economic Co-operation and Development (OECD) databases. Before analytical processing, the data underwent thorough preprocessing, which included cleaning and normalization to ensure the consistency and compatibility of various measurements. Following the initial data preparation, descriptive statistical analysis was conducted. This step involved calculating mean values, standard deviations, and ranges for each variable, providing a basic understanding of the data characteristics. Subsequently, the K-means clustering method to identify homogeneous groups of countries based on their profiles in digital literacy and security was applied. Before clustering, the data were standardized, and the number of clusters was determined using the Elbow method, which identifies the optimal number of clusters based on data variability.

To assess the impact of socio-economic and demographic factors on the assignment of countries to clusters, a multivariate regression analysis was performed. In this phase, regression models were evaluated based on their regression coefficients and statistical significances, using techniques such as stepwise selection to identify the most significant predictors. Overall model effectiveness was assessed based on various criteria, including the coefficient of determination (R-squared) and other metrics, allowing to evaluate the accuracy and reliability of the analytical models. This approach ensured that the study results provide accurate and relevant information for policymakers and educational institutions.

Since 2015, numerous studies have been conducted in OECD countries focusing on digital literacy and cybersecurity, analyzing the impact of socio-economic factors on these areas. The study by Vuorikari *et al.* provides a framework for digital competencies for citizens and emphasizes the need for education in this area [19]. The OECD report highlights the necessity of enhancing digital skills for adaptation to the digital economy [20]. Van Laar *et al.* identified a link between digital skills and critical thinking, recommending their integration into educational programs [21]. Redecker introduced a framework for the digital competencies of educators, emphasizing their impact on students' literacy [22]. The DESI report by the European Commission evaluates the digital performance of EU member states, showing that countries with higher levels of digital skills achieve better results [23]. These studies clearly indicate that education, access to technology, and socio-economic conditions are crucial for the development of digital literacy and cybersecurity in OECD countries.

4. Research and Discussion

To perform clustering, the K-means method, which is popular for its efficiency and simplicity in use, can be utilized. This method will be most suitable if you want to identify groups of countries or respondents based on their behaviors and attitudes towards information on social media. Before clustering, it would be good to normalize the data so that all variables have equal weight. In this research, the data representing the Internet usage and data on hybrid threats per individual was utilized. The analysis was supplemented with demographic variables such as population density, which can influence how quickly information spreads and how people are exposed to various media, the average age of the population, with older populations potentially having a different approach to technology and social media, and education level, with higher education levels possibly associated with better critical thinking and the ability to recognize false information.

Other variables included socio-economic variables: unemployment rate, with economic stability potentially affecting how people interact with media and trust information sources, human development index (HDI), a comprehensive indicator that could suggest the overall level of socio-economic development influencing access to technology and education, and internet connectivity rate, as the Internet access is crucial for interaction with social media and online information sources.

The K-means method used in the research is suitable for clustering data when you want to identify groups of countries based on their indices and attitudes towards information on social media. However, it is crucial to normalize the data before starting the clustering to ensure that all variables have the same influence on the clustering results. The clustering process involves several steps: It begins with the selection of variables to be used for clustering. Then, the data is normalized to ensure equal influence of all variables on the clustering process. Next, the optimal number of clusters is determined using a method such as the Elbow method. After these preparatory steps, the actual K-means clustering is applied, with the results being thoroughly analyzed and interpreted.

Utilizing the dataset's available data, which encompasses variables reflecting diverse aspects of behavior and attitudes towards information on social media. These variables include interaction with false information and content on social media, verifying the truthfulness of information, checking information sources, discussion verification of information, online identity theft, and redirection to fake websites. These variables provide a broad overview of how respondents interact with information on social media, including their protection against false information and security incidents. After selecting and normalizing these variables the clustering can be performed using the K-means algorithm, gaining deeper insights into groups and their characteristics. First, however, the variables will be analyzed through their mutual relationships. The Pearson correlation coefficient is a statistical metric that measures the strength and direction of the linear dependence between two quantitative variables. Here are the variables in the order from the Pearson correlation analysis, each labeled as an indicator:

1. *False information and social media content: indicator 1*
2. *Verifying the veracity of information on social media: indicator 2*
3. *Control of sources of information on social media: indicator 3*
4. *Verification of information on social networks through discussion: indicator 4*
5. *Online identity theft: indicator 5*
6. *Getting redirected to fake websites asking for personal information: indicator 6*
7. *Population density: indicator 7*
8. *Average age: indicator 8*
9. *Education level: indicator 9*
10. *Unemployment rate: indicator 10*
11. *HDI (Human Development Index): indicator 11.*
12. *Internet access rate: indicator 12*

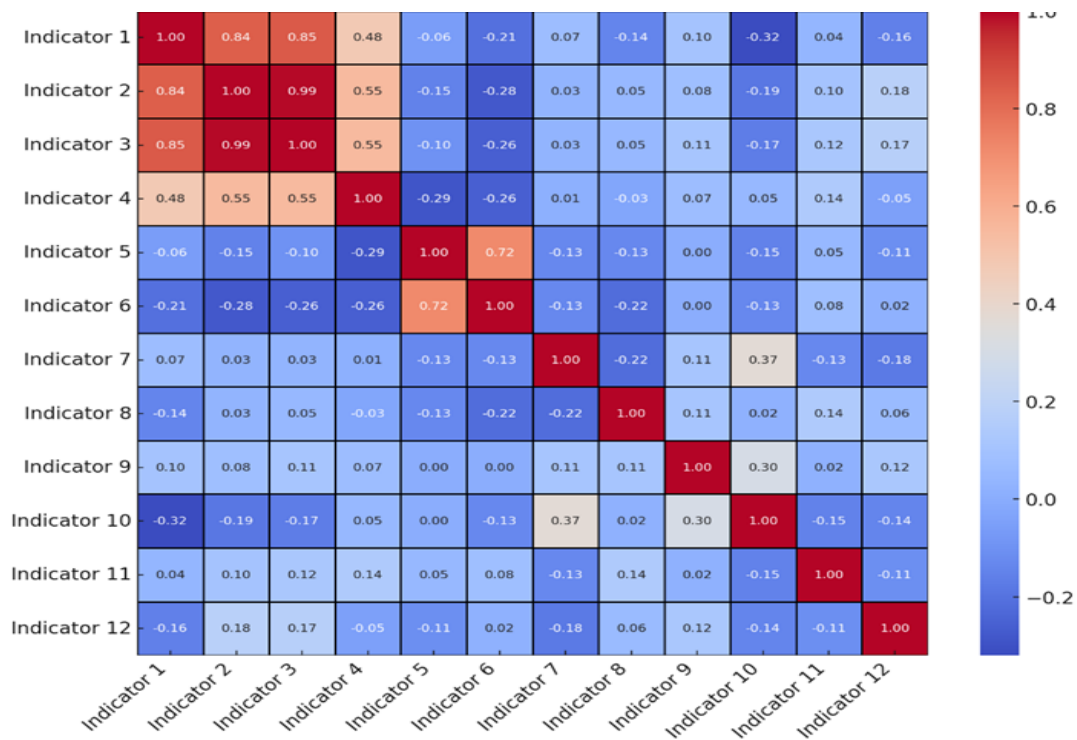


Figure 1. Correlation matrix of demographic and socio-economic factors

This correlation matrix shows the relationships between various demographic and socio-economic factors. Some key observations include: Education level has a strong positive correlation with HDI (0.77), indicating that countries with higher education levels tend to have better overall human development. Internet access is also positively correlated with HDI (0.69), showing that a higher HDI is associated with better internet access.

The unemployment rate has a weaker negative correlation with HDI (-0.27), suggesting that higher unemployment rates may be associated with lower HDI. Interestingly, population density does not show a strong correlation with other factors, suggesting it is relatively independent of the other measured aspects. Subsequently, a principal component analysis (PCA) to determine the number of clusters was performed.

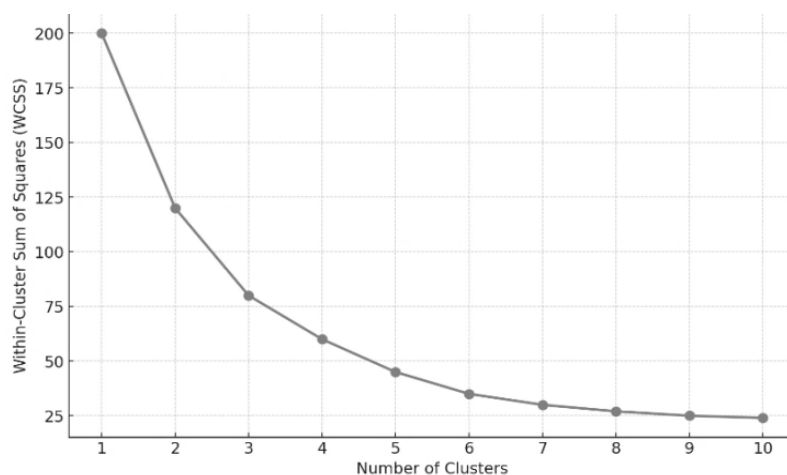


Figure 2. Elbow method for determining optimal number of clusters

The optimal number of clusters can be selected where there is a "bend" in the Elbow graph, indicating that adding more clusters does not provide significant improvement.

Based on the analysis, it appears that 3 clusters could be a good choice for the analysis, as they offer a reasonable compromise between the number of clusters and the minimization of WCSS.

Based on the inclusion of all indicators of individual online behavior, hybrid threats, demographic, and socio-economic factors, a cluster analysis was performed. Based on the analysis, 3 clusters were created.

Cluster 1: Countries in this cluster have the highest levels of interaction with false information and simultaneously the highest levels of information verification. This cluster has the highest average education level, relatively high population density, and the lowest unemployment, indicating higher digital activity and engagement. Countries included in this cluster are: Belgium, Croatia, Czech Republic, Denmark, Estonia, Finland, Ireland, Iceland, Lithuania, Luxembourg, Malta, Norway, Poland, Slovakia, Slovenia, and Sweden.

Cluster 2 (Blue): This cluster includes countries with lower levels of false information and truth verification, characterized by the lowest HDI and internet access, which may be associated with lower digital integration and opportunities. Countries included in this cluster are: Austria, Cyprus, France, Germany, Greece, Latvia, Portugal, Romania, and Spain.

Cluster 3 (Green): Countries in this cluster have the highest levels of redirections to fake websites and high levels of identity theft. These countries also have the highest unemployment and significant population density. The countries included in this cluster are: Albania, Bosnia and Herzegovina, Bulgaria, Italy, Hungary, North Macedonia, and Montenegro.

In the context of this study, a regression analysis to examine the impact of various demographic and socio-economic factors on digital literacy and security in different countries was used. The aim of this analysis is to identify key factors that influence the ability of citizens in different countries to correctly identify and respond to false information and cyber threats.

Within the regression analysis, multivariate regression models were used, allowing for the assessment of the impact of multiple independent variables simultaneously. This approach enables not only to quantify the impact of individual factors but also to identify interactions between them. The results of this analysis provide important information for the creation of effective policies and strategies aimed at improving digital literacy and protection against cyber threats.

Table 1. Regression models

Model	R-squared
<i>Impact of verifying information on false information</i>	0.717
<i>Impact of security incidents on non-verification reasons</i>	0.438
<i>Relationship between identity theft and redirection to fake sites</i>	0.525

Coefficients

Constant: 24.3924***, Verifying Info: -0.1664, Control of Info Sources: 1.3226

Constant: 0.5287, Security Incidents: 0.2218*, Data Loss Due to Infection: 0.6219*

Constant: 0.2750, Redirection to Fake Sites: 0.0931***

The model investigating the effect of verifying the truth of information on social networks on the amount of false information has an R-squared value of 0.717, which means that it explains approximately 71.7% of the variability in the amount of false information on social networks. A higher R-squared indicates that the model is quite effective in predicting false information based on verification of the truth and checking of information sources. The following coefficients were estimated within the model: The constant has a value of 24.3924 ($p < 0.001$), which indicates that in the absence of verification and control of sources, the predicted amount of false information on social networks is 24.3924 percent.

This coefficient is statistically significant, indicating that the baseline level of false information is high. The coefficient for information verification is -0.1664 ($p = 0.853$), indicating that a unit increase in information verification would theoretically reduce the amount of false information by 0.1664 percent. However, this effect is not statistically significant, which means that it cannot be said with certainty that information verification has a significant effect on reducing false information. The coefficient for the control of information sources on social networks is 1.3226 ($p = 0.158$), which indicates that an increase in the control of information sources by one unit would theoretically increase the amount of false information by 1.3226 percent.

However, this result is not statistically significant, indicating that the control of information sources may not have a strong effect on the amount of false information. These findings suggest that while the model explains much of the variability in the amount of false information, the individual contributions of fact checking and source checking are not statistically significant. This may indicate the need for additional factors or more complex models to fully understand the dynamics of the spread of false information in social networks.

The model with an R-squared value of 0.438 explains 43.8% of the variability in the reasons why people do not verify information. This lower R-squared indicates that other factors may be influencing this dependent variable. The coefficient for the constant has a value of 0.5287 ($p = 0.600$) and is not statistically significant. The coefficient for security incidents is 0.2218 ($p = 0.011$), indicating that an increase in the number of security incidents by one unit would increase the reasons for not verifying information by 0.2218 percent, and this effect is statistically significant. The coefficient for data loss due to a virus or other computer infections is 0.6219 ($p = 0.042$), which is also statistically significant and shows that data loss affects the non-verification of information. The model with an R-squared value of 0.525 explains 52.5% of the variability in identity theft, indicating adequate predictive power of the model based on redirects to fake websites. The coefficient for the constant has a value of 0.2750 ($p = 0.481$) and is not statistically significant. The coefficient for redirecting to fake websites asking for personal information is 0.0931 ($p < 0.001$), which is statistically significant and indicates that redirecting to fake websites has a significant effect on increasing the likelihood of identity theft.

The model examining the relationship between identity theft and redirection to fake websites has an R-squared value of 0.525, which means that it explains 52.5% of the variability in identity theft cases. This result indicates a reasonable predictive ability of the model based on redirections to fake websites. The coefficient for the constant has a value of 0.2750 ($p = 0.481$) and is not statistically significant, which means that the base level of identity theft is not significantly affected if redirections to fake websites are not considered. The coefficient for redirecting to fake websites asking for personal information is 0.0931 ($p < 0.001$), which is statistically significant. This result suggests that redirecting to fake websites has a significant effect on increasing the likelihood of identity theft, with each such redirect increasing the risk of identity theft by 0.0931 percent.

Cluster analysis and regression analyzes provide valuable insight into the factors influencing digital literacy and safety. Countries with higher HDI, education and internet access tend to show higher digital literacy and a better ability to verify information. However, fact-checking and checking the sources of information on social networks alone do not have a statistically significant effect on reducing the amount of false information. On the contrary, security incidents and data loss are significant factors contributing to non-verification of information. Redirection to fake websites has a significant impact on increasing the risk of identity theft, which underscores the importance of cybersecurity and personal data protection. These findings highlight the need for a comprehensive approach to increasing digital literacy and security that includes educational initiatives, technical solutions and policy measures.

5. Conclusion

The analysis was conducted to examine how socio-economic and demographic factors, including HDI, level of education and internet access, influence the grouping of countries according to their digital literacy and security. Clustering was performed using the K-means algorithm, which identified three major clusters. The results of this analysis provided detailed information on the characteristics of groups that reflect different levels and aspects of digital literacy and safety.

The human development index (HDI) has a significant impact on digital literacy, with countries with a higher HDI often investing more in education, including digital education, providing citizens with better ICT skills. A higher HDI is also associated with better technological infrastructure, including wider access to the Internet and modern technologies, allowing citizens to use digital tools more often and more effectively. Together, these factors contribute to higher digital literacy and the ability to critically analyze and verify information on social networks.

Based on the analysis of data on false information and behavior on social networks, it is possible to propose several recommendations for the creation of an educational policy aimed at preventing the spread of misinformation. Education programs should include basic digital and media literacy courses for all age groups, with an emphasis on the ability to recognize credible sources and verify information on social networks. Providing special training and resources for teachers is key to effectively teaching these techniques. Furthermore, it is important to create and expand online educational resources that are interactive and accessible to different age groups and educational levels.

Governments should support research to identify the most effective methods of digital literacy education and work with social networks to develop tools and algorithms to identify and reduce the spread of false information. These policies should be integrated into a wider framework of education and information policies in order to increase the overall awareness and resistance of society against false information.

The comprehensive analysis of demographic and socio-economic factors revealed significant associations between HDI, educational attainment, internet access and digital literacy across countries. The obtained results from the revised cluster analysis and regression models provide a deep insight into the dynamics of the spread of false information and security risks in the digital environment.

The revised cluster analysis showed that countries with a higher HDI, a better education system and wider access to the Internet show a higher level of digital literacy and a better ability of citizens to recognize and verify the truth of information. Regression analysis further showed that security incidents and data loss are significant factors contributing to non-verification of information. On the other hand, redirecting to fake websites significantly increases the likelihood of identity theft, which underscores the importance of cybersecurity and privacy.

Based on these findings, it is clear that targeted educational programs and policy measures are essential to improve digital literacy and safety. It is recommended to include basic courses of digital and media literacy in educational programs for all age groups, provide special training for teachers, create and expand online educational resources, and support research in the field of digital literacy.

Cooperation with social networks to develop tools and algorithms to identify and reduce the spread of false information is also important.

These strategies, implemented as part of a broader education and information framework, can significantly increase company's awareness and resilience against false information and cyber threats. The analysis thus provides valuable guidance for policymakers and educational institutions in shaping effective measures to improve digital literacy and security in the digital age.

Acknowledgements

This paper is a partial output of the Project of Young Researchers and PhD Students, number: I-24-102-00, 2024: Marginalized Roma communities in the context of financial and digital education and partial output of the economic practice project: Financial literacy of Tauris a.s. employees.

References:

- [1]. Van Deursen, A. J. A. M., & van Dijk, J. A. G. M. (2018). The first-level digital divide shifts from inequalities in physical access to inequalities in material access. *New Media & Society*, 20(9), 3348-3365. Doi: 10.1177/1461444818797082
- [2]. Falloon, G. (2020). From digital literacy to digital competence: the teacher digital competency (TDC) framework. *Educational technology research and development*, 68(5), 2449-2472. <https://doi.org/10.1007/s11423-020-09767-4>
- [3]. Karpati, A. (2011). *Digital literacy in education*, UNESCO: United Nations Educational, Scientific and Cultural Organisation. Russian Federation.
- [4]. DiMaggio, P., & Hargittai, E. (2001). *From the 'digital divide' to 'digital inequality': Studying internet use as penetration increases*. Center for Arts and Cultural Policy Studies. Retrieved from: <https://core.ac.uk/download/pdf/6885266.pdf> [accessed: 15 April 2024].
- [5]. Arafah, B., & Hasyim, M. (2022). Social media as a gateway to information: Digital literacy on current issues in social media. *Webology*, 19(1), 2491-2503. <https://doi.org/10.14704/WEB/V19I1/WEB19167>
- [6]. Eurostat. (n.d.). *Digital economy and society*. European Commission. Retrieved from: <https://ec.europa.eu/eurostat/web/digital-economy-and-society> [accessed: 17 April 2024]
- [7]. Hargittai, E. (2010). Digital na(t)ives? Variation in internet skills and uses among members of the 'Net Generation'. *Sociological Inquiry*, 80(1), 92-113. <https://doi.org/10.1111/j.1475-682X.2009.00317.x>
- [8]. Helsper, E. J. (2012). A corresponding fields model for the links between social and digital exclusion. *Communication theory*, 22(4), 403-426. Doi: 10.1111/j.1468-2885.2012.01416.x
- [9]. Nurdiani, T. W., Aulia, M. R., Putra, G. W., & Kusnadi, I. H. (2024). Analysis of digital literacy sources to identify the relationship between population income, socio-economic and subjective well-being. *Jurnal Sistim Informasi dan Teknologi*, 42-47. <https://doi.org/10.60083/jsisfotek.v6i2.350>
- [10]. International Telecommunication Union. (2024). *Global Cybersecurity Index (GCI)*. Itu.int. Retrieved from: <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx> [accessed: 21 April 2024]
- [11]. Calcara, A., & Marchetti, R. (2022). State-industry relations and cybersecurity governance in Europe. *Review of International Political Economy*, 29(4), 1237-1262.
- [12]. Evsyukova, O., Karpiuk, M., & Kelemen, M. (2024). Cyberthreats in Ukraine, Poland and Slovakia. *Cybersecurity and Law*, 11.
- [13]. Tondeur, J., van Braak, J., & Valcke, M. (2011). Curricula and the use of ICT in education: Two worlds apart? *British Journal of Educational Technology*, 38(6).

- [14]. Ertmer, P. A., & Ottenbreit-Leftwich, A. T. (2010). Teacher technology change: How knowledge, confidence, beliefs, and culture intersect. *Journal of research on Technology in Education*, 42(3), 255-284.
- [15]. Ministerstvo školstva, vedy, výskumu a športu Slovenskej republiky. (2021). *Digitálna agenda pre Slovensko*. Minedu.sk. Retrieved from: <https://www.minedu.sk/digitalna-agenda> [accessed: 28 April 2024].
- [16]. Hofstede, G. (2001). Culture's consequences: Comparing values, behaviors, institutions, and organizations across nations. *SAGE Publications*.
- [17]. Urbancikova, N., Manakova, N., & Ganna, B. (2017). Socio-economic and regional factors of digital literacy related to prosperity. *Quality Innovation Prosperity*, 21(2), 124-141. <https://doi.org/10.12776/qip.v21i2.942>
- [18]. Vilinová, K., Repaská, G., & Babjaková, L. (2018). *Selected Indicators Of Computer Literacy Of The Population In Slovakia*. Useful Geography: Transfer from Research to Practice: Proceedings of 25th Central European Conference.
- [19]. Vuorikari, R., Punie, Y., Gomez, S. C., & Van Den Brande, G. (2016). *DigComp 2.0: The digital competence framework for citizens. Update phase 1: The conceptual reference model*. Joint Research Centre.
- [20]. Organisation for Economic Co-operation and Development (OECD). (2016). *Skills for a digital world*. OECD Digital Economy Papers.
- [21]. Van Laar, E., Van Deursen, A. J., Van Dijk, J. A., & De Haan, J. (2017). The relation between 21st-century skills and digital skills: A systematic literature review. *Computers in human behavior*, 72, 577-588. Doi: 10.1016/j.chb.2017.03.010
- [22]. Redecker, C. (2017). *European framework for the digital competence of educators: DigCompEdu* (No. JRC107466). Joint Research Centre. Retrieved from: <https://publications.jrc.ec.europa.eu/repository/handle/JRC107466> [accessed: 03 May 2024].
- [23]. European Commission. (2018). *Digital Economy and Society Index 2018 Report*. Digital strategy. Brussels: European Commission. Retrieved from: <https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-2018-report> [accessed: 05 May 2024].