Claudio Melchior*
Urszula Soler**

Security of Personal Data in Cyberspace in the Opinion of Students of the University of Udine

Abstract

The escalating concerns surrounding personal data security in cyberspace necessitate a comprehensive examination of user awareness, attitudes, and behaviours. This study, conducted among University of Udine students, delves into the multifaceted dimensions of personal data security, exploring aspects such as perceptions and behaviours related to privacy, network security, and legal compliance. The research objectives involve assessing respondents' awareness of data transfer on the network, their general concerns about cyber risks, and the coherence between awareness, concern, and actual online behaviour. A convenience sample of 518 predominantly young respondents was gathered through an online questionnaire. Results reveal a noteworthy disparity between declared awareness and actual concern, leading to a „privacy paradox". While respondents express awareness of data transfer, their specific concern is limited, predominantly focusing on commercial aspects rather than acknowledging broader cybersecurity threats. This discordance extends to online behaviour and the predominant use of devices such as smartphones, which are simultaneously the most used by respondents but also perceived to have the greatest data loss and the least possibility of implementing data protection actions. The findings underscore the critical need for ongoing cybersecurity education, particularly targeting younger populations, to bridge the gap between theoretical awareness

* Assoc. Prof. Claudio Melchior, PhD, Dipartimento di Lingue e Letterature, Comunicazione, Formazione e Società, e-mail: claudio.melchior@uniud.it, ORCID: 0000-0002-6124-4717.
** Assoc. Prof. Urszula Soler, PhD, Institute of Political Science and Public Administration, The John Paul II Catholic University of Lublin, e-mail: urszula.soler@kul.pl, ORCID: 0000-0001-7868-8261.

and practical implementation of secure online practices. This study prompts further investigation into diverse cultural contexts, proposing a shared model for technological education across European societies to foster secure behaviours in the digital landscape.

Key words: personal data, security, cybersecurity, „privacy paracox", sociological research, technological education

Introduction

The issue of personal data security has been a subject of interest for researchers worldwide for many years. Its significance has become even more critical with the development and widespread use of the Internet. The highly dynamic growth of mobile phones and the popularity of smartphones in the 21st century have also contributed to this. Personal data security in cyberspace constitutes a broad field focusing on safeguarding information that identifies or can be linked to specific individuals. It is most commonly raised in a few key aspects. The first is privacy, as securing personal data is crucial for protecting people's privacy. Cyberspace is a particular realm where numerous threats to privacy exist. This includes identity theft, unauthorised data access, or surveillance. Equally important is network security, primarily centred on preventing attacks on computer systems that may lead to data breaches. Such attacks can originate from hackers, cybercriminals, or even state actors.

The second important aspect in which the security of personal data in cyberspace is highlighted is compliance with legal regulations. There are regulations governing the collection, storage, and processing of personal data, such as the GDPR[1] in the European Union. This issue involves matters related to legal compliance and the need to ensure that companies and institutions adhere to the relevant regulations. In cyberspace, this is regulated by the NIS Directive[2] (Network and Information Security Directive) and its newer version, NIS2[3] (Network and Information Security Directive 2). They primarily focus on ensuring the security of networks and computer systems in the European Union, aiming to enhance resilience against cyberattacks and prevent cybersecurity incidents. Both directives, NIS and NIS2, aim to increase

1 *General Data Protection Regulation*, https://uodo.gov.pl/404 [access: 28.12.2023].
2 *Network and Information Security Directive*, https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new [access: 28.12.2023].
3 *Network and Information Security Directive 2*, https://eur-lex.europa.eu/eli/dir/2022/2555 [access: 28.12.2023].

the EU's resilience to cyberthreats, establish security standards for entities critical to society, and strengthen cooperation and information exchange among member countries in the field of cybersecurity[4].

As regards the cybersecurity of personal data in cyberspace, awareness and education of individuals are also crucial. Internet users must be aware of cyberthreats and know how to protect their personal data[5]. Implementing cybersecurity education is becoming increasingly important, and more countries are taking appropriate actions here. Simultaneously, there is a need for the development of technological safeguards. Various technologies aimed at securing data, such as encryption, authentication systems, & network security, are being developed. Efforts related to risk management are also undertaken, including security audits, data protection policies, and proper procedures in case of data breaches.

Summarising the introduction to this article, personal data security in cyberspace is a complex issue encompassing multiple areas. With technological advancements, this matter is becoming increasingly critical for all internet users and corporations processing personal data. Therefore, conducting research in this area, including sociological research about people's awareness

4 In the realm of cybersecurity, also consider: M. Karpiuk, *Tasks of the Minister of National Defence in the area of cybersecurity*, „Cybersecurity and Law" 2022, no. 1; M. Czuryk, *Restrictions on the Exercising of Human and Civil Rights and Freedoms Due to Cybersecurity Issues*, „Studia Iuridica Lublinensia" 2022, no. 3; M. Karpiuk, *The obligations of public entities within the national cybersecurity system*, „Cybersecurity and Law" 2020, no. 2; idem, *Crisis management vs cyber threats*, „Sicurezza, Terrorismo e Societa" 2022, no. 2; M. Czuryk, *Supporting the development of telecommunications services and networks through local and regional government bodies, and cybersecurity*, „Cybersecurity and Law" 2019, no. 2; M. Karpiuk, *The Local Government's Position in the Polish Cybersecurity System*, „Lex Localis – Journal of Local Self-Government" 2021, no. 3; M. Czuryk, *Cybersecurity as a premise to introduce a state of exception*, „Cybersecurity and Law" 2021, no. 2; A. Bencsik, M. Karpiuk, *Cybersecurity in Hungary and Poland. Military aspects*, ibidem 2023, no. 1; I. Hoffman, M. Karpiuk M., *The local self-government's place in the cybersecurity domain. Examples of Poland and Hungary*, ibidem 2021, no. 1; M. Karpiuk, A. Makuch, U. Soler, *The role of the Cybersecurity Strategy of the Republic of Poland in ensuring cybersecurity*, „Polish Political Science Yearbook" 2023, vol. 52, no. 3, p. 155–163; M. Karpiuk, *Cybersecurity as an element in the planning activities of public administration*, „Cybersecurity and Law", no. 1; M. Adamczyk, M. Karpiuk, U. Soler, *The use of new technologies in education – opportunities, risks and challenges in the times of intensive intercultural change*, „Edukacja Międzykulturowa" 2023, no. 4; A. Bencsik, M. Karpiuk, *The legal status of the cyberarmy in Hungary and Poland. An overview*, „Cybersecurity and Law" 2023, no. 2.

5 K. Chałubińska-Jentkiewicz, *Cyberodpowiedzialność. Wstęp do prawa cyberbezpieczeństwa*, Toruń 2023.

and behaviour, is crucial. These efforts aim to ensure that actions taken in the realm of personal data security in cyberspace are targeted and coherent.

Current State of Research

The issue of internet security, including personal data protection, has been extensively explored by numerous researchers worldwide. Bruce Schneier, an acclaimed cryptographer and expert in cybersecurity, stands out among the prominent figures. He has authored several books on security[6], including those focusing on personal data protection, such as „Protect Your Macintosh"[7], „E-Mail Security"[8], and „Beyond Fear: Thinking Sensibly about Security in an Uncertain World"[9]. Equally significant are the contributions of Kevin Mitnick, formerly known as a notorious hacker and now an expert in security[10]. Another notable figure is Daniel Solove, a law professor at George Washington University Law School, renowned for his work on privacy in the digital age. His book „Nothing to Hide: The False Tradeoff between Privacy and Security"[11] delves into the relationship between privacy and data security.

Additionally, the literature review regarding the impact of data collection on privacy and society is noteworthy. Shoshana Zuboff's book „The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power"[12], discusses the influence of data collection on privacy and society. Edward Snowden's „Permanent Record" is another significant work where he shares his experiences with the NSA, raising concerns related to privacy

6 B. Schneier, *Applied Cryptography*, New Jersey 1996; idem et al., *The Twofish Encryption Algorithm*, New Jersey 1996; idem, D. Banisar, *The Electronic Privacy Papers*, New Jersey 1997; B. Schneier, *Secrets and Lies*, New Jersey 2000; idem, *Schneier on Security*, New Jersey 2008; N. Ferguson, B. Schneier, T. Kohno, *Cryptography Engineering*, New Jersey 2010; B. Schneier, *Liars and Outliers: Enabling the Trust that Society Needs to Thrive*, New Jersey 2012.
7 Idem, *Protect Your Macintosh*, Berkley 1994.
8 Idem, *E-Mail Security*, New Jersey 1995.
9 Idem, *Beyond Fear: Thinking Sensibly about Security in an Uncertain World*, New York 2003.
10 K. Mitnick, R. Vamosi, *The Art of Invisibility*, Boston 2017; K. Mitnick, W.L. Simon, *Ghost in the Wires: My Adventures as the World's Most Wanted Hacker*, Boston 2011; eidem, *The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders, and Deceivers*, New Jersey 2005; K. Mitnick, *The Art of Deception: Controlling the Human Element of Security*, New Jersey 2002, Paperback.
11 D. Solve, *Nothing to Hide: The False Tradeoff Between Privacy and Security*, Yale 2011.
12 S. Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, New York 2019.

and security in the digital era[13]. In exploring privacy in the digital age, Julia Angwin's[14] „Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance" is also worth mentioning.

In the realm of sociology and the study of technology's impact on society, significant contributions come from Zeynep Tufekci. Among her notable works is „Twitter and Tear Gas: The Power and Fragility of Networked Protest"[15], where the author analyses the role of social media in contemporary social movements. Directly relevant to the subject of this article, Danah Boyd is an influential researcher focusing on technology, youth, and society. Her book „It's Complicated: The Social Lives of Networked Teens"[16] explores how young people use technology and its influence on their social lives. Addressing the impact of technology on social life are also such researchers as Safiya Noble, whose work concentrates on analysing biases and inequalities in internet search engines and their societal effects[17]. In the Polish context, notable researchers include Aleksandra Jasińska-Kania, who delves into social aspects of technology, and Urszula Soler, whose work encompasses studies on technology's impact on social life[18].

13 E. Snowden, *Permanent Record*, Macmillan, New York 2019.

14 J. Angwin, *Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance*, New York 2014.

15 Z. Tufekci, *Twitter and tear gas: the power and fragility of networked protest*, New Haven 2017.

16 D. Boyd, *It's Complicated: The Social Lives of Networked Teens*, Yale 2014.

17 S. Noble, *Algorithms of oppression: how search engines reinforce racism*, New York 2018.

18 J. Ejdys, U. Soler, *The society's attitude toward 5G technologies – a case study of Poland*, „Technological and Economic Development of Economy" 2023, vol. 29, no. 5, p. 1539–1558; U. Soler, *Social perception of 5G technology*, „Rocznik Instytutu Europy Środkowej" 2022, R. 20, z. 1, p. 103–120; eadem, M. Busiło, *Oswajanie z technologią. Na przykładzie elektryfikacji Wielkiej Brytanii i technologii 5G*, „Przegląd Elektrotechniczny" 2019, no. 12, p. 97–100; U. Soler, *Technologia jako narzędzie wzmacniania więzi społecznych*, „Zeszyty Naukowe Politechniki Śląskiej". Ser. „Organizacja i Zarządzanie" 2018, vol. 113, p. 273–286; eadem, *The Role of Network Technologies in European Cybersecurity* [in:] *The Role of Cybersecurity in the Public Sphere – The European Dimension*, eds. K. Chałubińska-Jentkiewicz, I. Hoffman, Maribor 2022, p. 47–58; U. Soler, M. Busiło, *Education of society as a tool to counteract disinformation in implementing new technologies. On the example of 5G mobile telecommunications network and Warsaw sewage system* [in:] *Proceedings of the International Conference „Applications of Electromagnetics in Modern Engineering and Medicine" June 9–12, 2019, Janów Podlaski, Poland*, New York 2019.

Research objectives and bias

The objective of our research work is to analyse (research questions):

– respondents' awareness of the transfer of data on the network;

– their concern (or disinterest) concerning the transfer of data and „cyber risks" in general;

– the coherence between awareness and concern on the one hand and the actual behaviour enacted on the network on the other.

In particular, we expect to find a large gap between:

1) declared awareness of risks and the actual awareness of them;

2) the declared „defensive behaviours" and the actual behaviours enacted.

Considering the impact of privacy concerns on privacy behaviour, it can be stated that one will comply. However, research suggests that this occurs rarely. Only in cases where there is a discrepancy between the threats to people's privacy and their privacy behaviours. This phenomenon is known as the „privacy paradox", a term coined by Barry Brown[19]. Using supermarket loyalty cards does not align with the concerns of customers who might use the services.

Methods

The data present a convenience sample collected through a questionnaire of 38 questions (mainly closed-ended questions) distributed online from the Public Relations Office of the University of Udine (Italy). Therefore, more than three-quarters of the 518 respondents are university students (79,7%) aged between 18 and 25 (75,2% of the sample).

We are therefore aware of certain biases in the constitution of this analysis group: 1) the method of constituting the group of respondents (convenience sample) does not allow us to obtain a representative statistical sample and we are therefore in the context of a pilot study; 2) since the selection procedure started from the primary relationships of a group of university students, this is indicative of a higher socio-cultural level than would have been obtained with a random selection procedure; 3) the use of the Internet is also overestimated

19 *The Privacy Issue. Decoding the Privacy Paradox*, 2021, https://theprivacyissue.com/privacy-and-society/decoding-privacy-paradox [access: 28.06.2023].

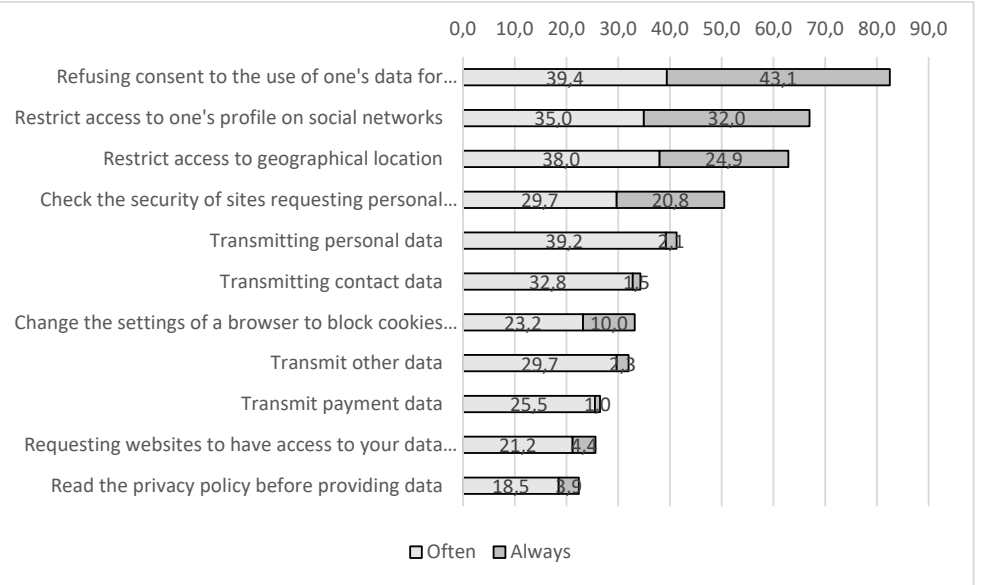
with respect to the general population because a) the online diffusion mode acted as a barrier of access to those who are not actually connected; b) the possibility of deciding whether or not to take part in the questionnaire also depended on the topic addressed; c) the sample is concentrated in the youngest age brackets, which are known to be the most „connected" population brackets (in fact, as we shall see, all our youngest respondents are „hard users", especially of smartphones, which they use every day in multiple modes).

Respondents and their use of the Internet and social media

The 518 respondents (79,7% of whom, as mentioned, are university students) are predominantly female (62,7%). They are concentrated, as mentioned, in the younger age groups: in particular, half of the respondents are aged between 22 and 25 (52,5%) and another 22,7% are aged between 18 and 21. Overall, 83,9% of the respondents are under 30 years of age. They are all exceptionally connected to the net. They state that they use the Internet „every day" (99,6%) and do so overwhelmingly using their smartphones (78,1%): only 18,4% of respondents (also) use computers, and the only alternative device mentioned in the answers, the tablet, is residual (3,2%).

When asked what activities they do on the Internet, they answered that the most frequent activity was consulting social networks (47,9% said they did it „always"). This is closely followed by the use of the network to contact and exchange messages with friends and relatives (83,7%) and the use of the network for entertainment purposes (82,6%). However, in these two cases, the prevailing answers are more nuanced and the number of answers „often", as opposed to „always", increases. The detailed data are presented in Graph 1.

The hyper-connectedness to the network of this group of respondents, and in particular their exposure to social networks, is reaffirmed by the answer to a specific question on the frequency of use: more than eight out of ten respondents stated that they used social networks „every day" (82,4%) even though, as we have seen, this is a predominantly passive use, since the active publication of content concerns only one-third of the sample (see Graph 1).



Source: based on the authors' own research.

Graph 1. Most frequent actions on the Internet (only answers „often" and „always")

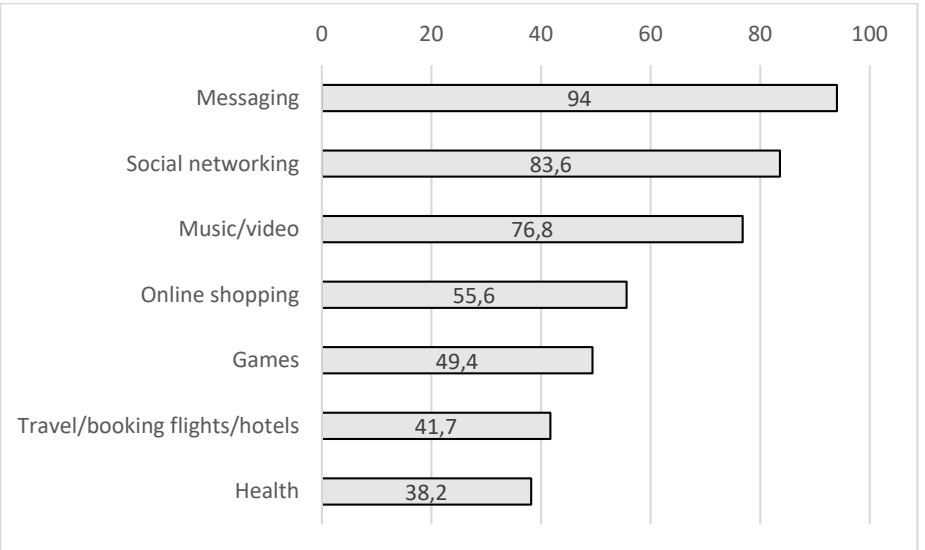
The frequency of use of social networks is not influenced by the occupation of the respondents (it is independent of whether they are students or workers) nor by their gender. On the contrary, it is significantly (inversely) correlated with age[20]: the frequency of use of social networks goes down as age goes up, as does, in general, all the activities on the network that we analysed. Constructing an „activity index" (a continuous index obtained by summing the individual answers of the respondents to the questions on the frequency of the various activities), we can see that the youngest are clearly the most active on the Internet and in the use of social media[21]. The same kind of relationship can be seen between the activity index and employment, with students overall more active on the net and social media than their colleagues who work[22].

The influence of gender and occupation is only noticeable in some specific uses of social media, such as the habit of using social media to keep in touch and to follow brands/famous people (which is more frequent among women,

20 Age – social use: χ^2 (21, N = 516) = 76.3, p = .000.
21 Age – activity index: τ_b = -.137, p<.01 (N = 516).
22 Occupation – activity index: τ_b = -.112, p<.01 (N = 516).

students and younger people)[23]. Posting content is also more frequent among women, while respondents who are still students use social for entertainment more than their working colleagues.

The 518 respondents claim to have 1287 accounts open on the various social networks (for an average of two and a half active accounts each), with Instagram taking the lion's share, with 446 accounts: 86,1% of respondents, therefore, have an Instagram account. This is followed at a notable distance by Facebook (340 accounts; 65,6% of respondents) and further behind by Skype (203; 39,2%), TikTok (154; 12%) and Snapchat (118 accounts; 9,2%). Various other socials mentioned (such as Reddit, Linkedin, BeReal, Tumblr, and Discord) added together do not total more than 2% of the responses. As shown below, consultation of social networks predominantly takes place through smartphones. Social network applications (second only to messaging apps) are installed on the smartphones of respondents (see Graph 2).



Source: based on the authors' own research.

Graph 2. Applications installed on the smartphone

23 Gender – use of social media to keep in touch: χ^2 (3, N = 514) = 13,467, p = .004. Gender – use of social media to follow brands/personalities: χ^2 (3, N = 514) = 18,852, p = .000. Gender - social publishing content: χ^2 (3, N = 514) = 18,399, p = .000. Occupation – use of social media to keep in touch: χ^2 (3, N = 516) =14,833, p = .002. Occupation – use of social media to follow brands/personalities: χ^2 (3, N = 516) = 25,701, p = .000. Age – use of social media to keep in touch: χ^2 (21, N = 516) =89,993, p = .000. Age – use of social media to follow brands/personalities: χ^2 (21, N = 516) = 75,247, p = .000. Occupation – use of social media for entertainment: χ^2 (3, N = 516) = 34,059, p = .000.

Awareness and concern about risks

Substantially all respondents declare themselves aware of the fact that, by using the Internet, they „surrender" personal data to the outside world (98,8%). The question concerning the specific awareness related to the existence and functioning of „cookies" provides only slightly lower percentages (91,9% of respondents saying they are „aware"). So, theoretically, at least, our respondents (irrespective of age, gender, occupation or level of activity on the net) are aware of the transfer of their data on the net. Once, however, we jump to investigate not awareness (declared) but concern about this phenomenon (always stated), the picture clearly changes.

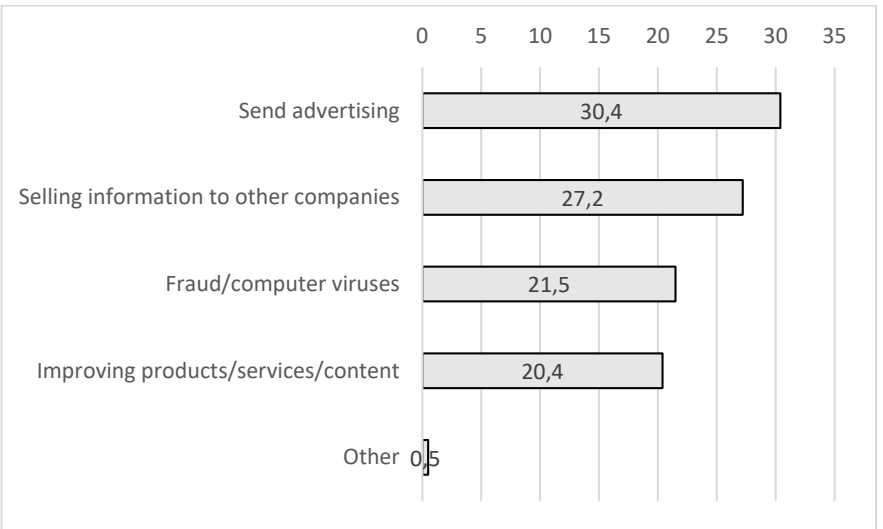
To the direct question „Are you worried about the data you give away via the Internet?", the respondents split closely in half: 50,4% say they are „quite" or „very" worried, while the remaining 49,6% are „a little" or „not at all" concerned. If we then observe that the large majority of the sample responds using the less clear-cut dimensions of „a little" (44%) and „quite a lot" (41,5%), this leads us to think that the actual concern is even less high than this split in half might suggest. After all, only 14,5% of the whole sample expresses a clear-cut opinion, and those who say they are „very" concerned account for only 8,9%, not even one respondent in ten. Interestingly, the level of concern, which is correlated neither with gender, age or occupation, is instead correlated (inversely) with the rate of activity on the net: the greater the Internet use, the lower the level of privacy concern. But this correlation, while significant, is not very strong[24]. In general, therefore, the low level of concern is widespread and runs throughout the sample.

This low level of stated concern is related to the specific perception of risks involved in the transfer of personal data. Indeed, respondents associate these risks almost exclusively with the commercial and advertising sphere (Graph 3).

As can be seen, the idea is that data transferred externally may only involve the receipt of „personalised" advertisements (the first two dimensions mentioned, the most frequent in which we have re-grouped with a content analysis of the open-ended answers provided by the respondents to the question) or also used for a purpose that can be considered „positive", such as the improvement of products and services. The dimension of scams and computer viruses stands out within the answers as the only clearly „negative"

24 Concern level – activity rate: $\tau_b = -.096$, $p<.01$ (N = 518).

or „risky" dimension of data transfer to the outside world. A dimension that is in any case „private" and „residual". It can be considered private because frauds and viruses are phenomena that can be associated with the fraudulent behaviour of single individuals or single groups, not with the overall behaviour of the data dissemination system (in other words, handing over data on the network, e.g., to a social network, is declared risky only in the event that some external individual or group 'steals' these data and uses them for its fraudulent purposes; the direct transfer of data to the social network does not, therefore, seem to be perceived as risky in itself: at most, it leads to receiving a different kind of publicity). It is „residual" because, in any case, it is a dimension indicated by only one out of five respondents, the same percentage of respondents who say they perceive the risk of „cyberattacks" on the network as „high". Only a small number of responses, which cannot be grouped into the four dimensions indicated in Graph 3, mention different, systemic and not merely commercial uses of the data transferred on the network (0,5% of responses summarised in Graph 3 as „other"). These answers speak of the „profiling" or „observation" of persons and communities by „companies" or „government bodies", of „censorship", of the „creation of needs" that one does not need, emphasising the fact that these data „have great value" (and are therefore retained) and that their collection may in any case be exposed to the risk that they may be „hacked" or be available to „disloyal insiders". But, as mentioned, these responses can be counted on the fingers of two hands.



Source: based on the authors' own research.

Graph 3. How could data collected by third parties be used?

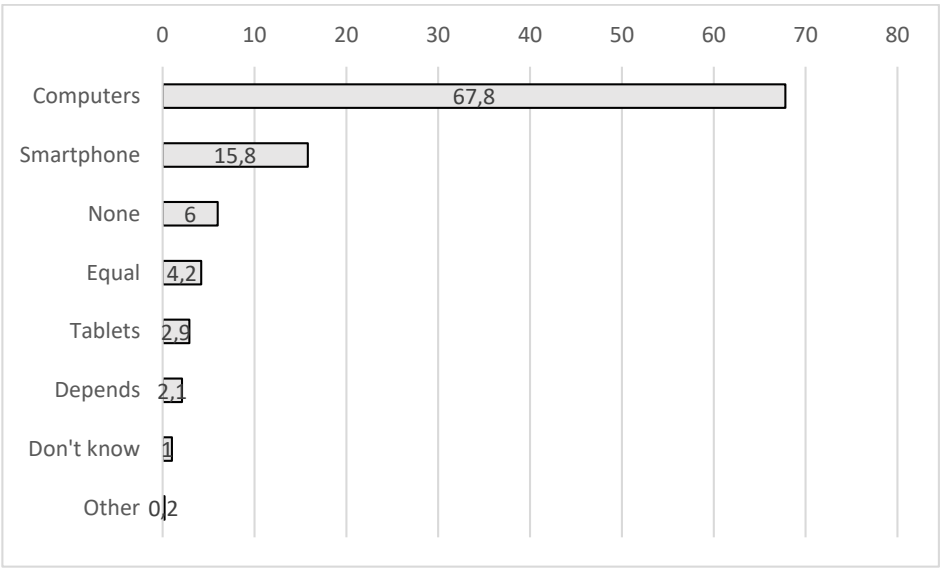
Our interpretation leads us to think that in reality, beyond the respondents' self-declared „awareness" of the phenomenon of the transfer of their data, the level of concern related to this transfer is very low (also because, as seen, it is almost exclusively associated with the use of data for commercial purposes). In fact, their perception of the risk, whatever it may be in an absolute sense, contrasts with two other indications that emerge from the questionnaire:

– the devices that are reported to be most „risky" concerning data loss are the devices that respondents use most frequently;

– the network „environments" that are declared „riskiest" are the environments that respondents frequent the most.

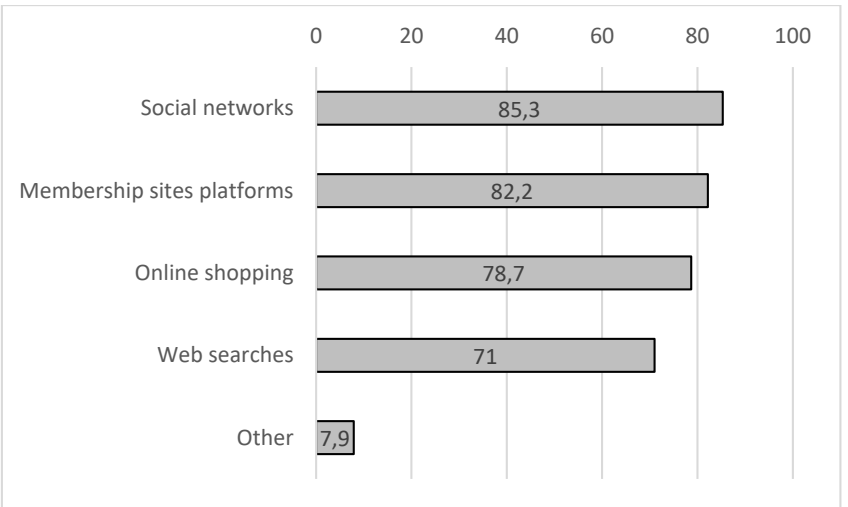
When asked, „In your opinion, which device is the most secure with regard to the protection of personal data?", 67,8% of respondents say it is the computer, while the smartphone is secure for only 15,8% of respondents. But we noticed that the respondents overwhelmingly use the smartphone (78,1%), i.e., the „least secure" device, while only 18,4% of respondents use the „most secure" computer. The remaining respondents, i.e., the 16,4% of respondents who indicate neither computer nor smartphone as the „most secure" devices, are divided between 10,2% who answer that „no device" is secure or that they are all „equally" secure or insecure, and the remaining 2,1% who indicate more specific conditions. According to them, security/insecurity depends on the use of the device, the amount and quality of the data contained in the device, antivirus software, the operating system, the browser used, the configuration of the device, whether or not one is „logged in" with an account, the „care taken" or the individual's competence in this regard. But as mentioned, these responses are absolutely residual in absolute numbers (Graph 4).

When we move from analysing devices to analysing activities on the net, we can see that the activity considered to be the riskiest for 85,3% of respondents is precisely frequenting social networks, which, as we have seen, was the most frequent activity carried out by our respondents on the net (Graph 5).



Source: based on the authors' own research.

Graph 4. In your opinion, which device is most secure with regard to data protection?



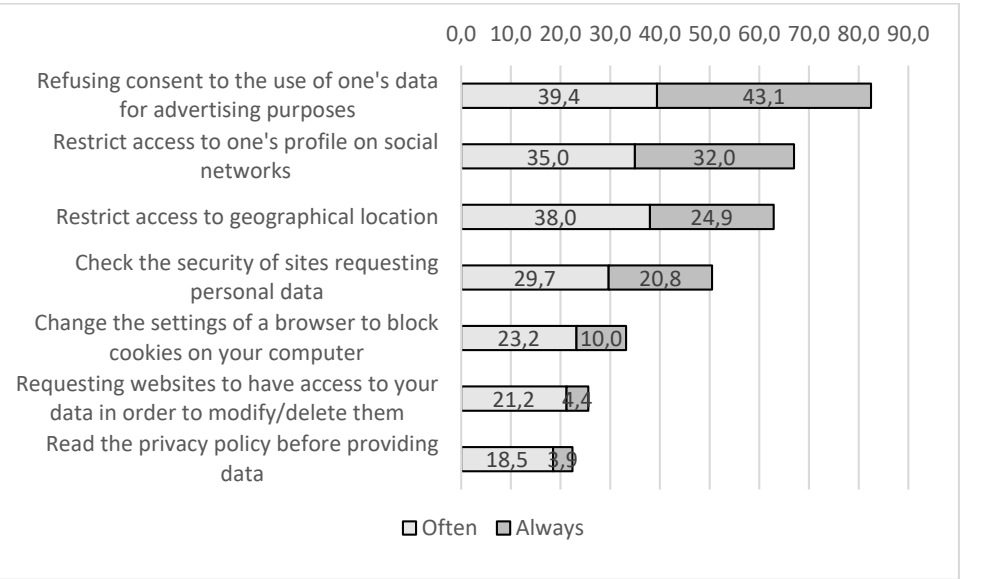
Source: based on the authors' own research.

Graph 5. In your opinion, what activities on the Internet lead to data recovery by outsiders?

Behaviour and „defensive" actions

Even the answers to the questions that directly address the frequency with which respondents perform actions on the net that can be considered on the one hand 'safe' and on the other hand „dangerous" with respect to the protection of privacy provide data that we can consider contradictory to each other.

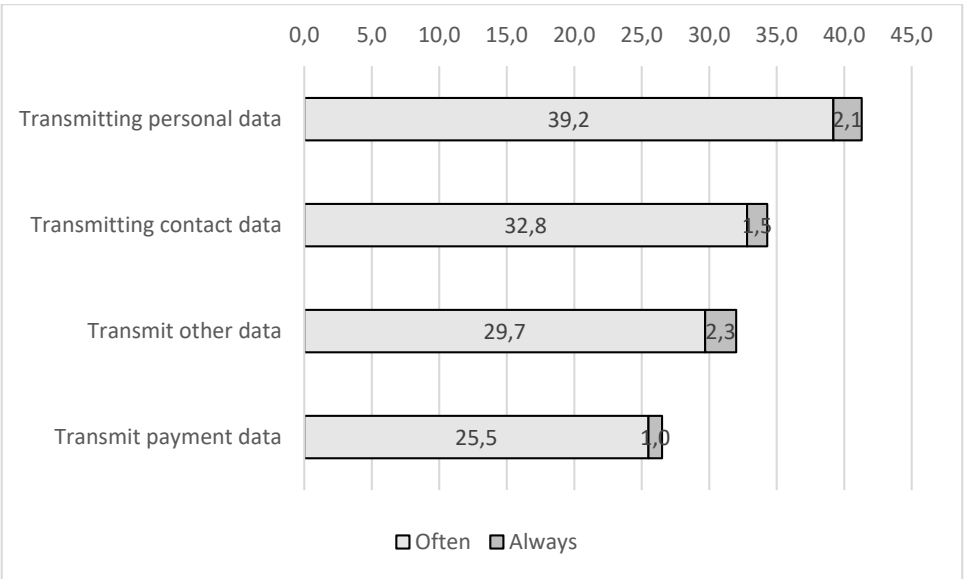
On the one hand, actions to protect one's privacy seem to be quite widespread: 82,5% of respondents tell us that they „always" (43,1%) or „often" (39,4%) refuse to consent to the use of their data for advertising purposes; lower percentages, but still significant, for those who say they „restrict access to their profile on social networks" and „restrict access to geographical location" (67% and 62,9% respectively) and half of the sample declare to „check the security of sites that request personal data". Only „changing a browser's settings to block cookies on your computer", „requesting websites to have access to your data to modify/delete it" and „reading the privacy policy before providing data" provide responses below 50% of the sample (Graph 6).



Source: based on the authors' own research.

Graph 6. Most frequent „defensive" actions on the network

Looking at the data of these „defensive" actions, we could conclude that the respondents are rather careful about their privacy. However, we then find that more than one-third of the sample declares that they „often" or „always" transmit personal data of various kinds[25] (Grapt 7). The frequency with which respondents engage in these „defensive" activities or, vice versa, consciously transmit personal data over the network is influenced neither by age, gender or occupation.



Source: based on the authors' own research.

Graph 7. Most frequent data transmission

Even the specific question on cookie consent behaviour provides a polarised situation: half of the sample declare that they only accept the necessary cookies or in any case choose their own personalised configuration; but we find also two groups who expressly declare that they refuse (25,1%) or, on the contrary, accept cookies without reading the information (23,7%). These two „extreme" groups, curiously enough, when isolated and compared do not

25 The same typology of contradiction concerning the „high perception of declared risk" as opposed to „low implementation of defensive behaviour" emerges from other researches, again conducted on highly digitised young university students, on the topic of climate change. See C. Melchior, *News and climate change: opinions, degree of information and awareness of Italian university students* [in:] *Communities, technology and this moment*, eds. L. Stillman, M. Anwar, C. Rhinesmith, Melbourn 2021, p. 124–138.

show significant correlations either with the frequency of use or with the rate of activity on the network, which remains similar. Those who reject cookies have only a (slightly) greater propensity[26] to implement the other defensive activities shown in Graph 6, while no significant differences are found in the fact that they consciously transmit their data over the network.

To better analyse this contradictory data, we constructed two indices called the „defensive index" and the „non-defensive index", obtained by summing up the respondents' statements on how much they used to carry out „defensive actions" shown in Graph 6 and a „non-defensive" index obtained by summing up their actions of info transmission (Graph 7). These continuous indices were then divided into four bands (low, medium-low, medium-high and high) in order to isolate those respondents who were most 'contradictory' about their actions on the network: on the one hand, those who have both indices ('defensive' and 'non-defensive') high (21% of the sample); and on the other hand, those who have both indices low (20%). Table 1 shows by key indications the main differences found between these two contradictory groups.

Table 1. Analysis of the contrasting characteristics of the most „contradictory" respondents

Low „defensive" and „non-defensive" index	High „defensive" and „non-defensive" index
more males	more females
plus the very young (18–21 years)	plus 22 to 30 years old
more concerned about the data they give out on the internet	less concerned
they refuse consent to cookies the least, and are also the ones who „accept without reading" the most	they refuse consent to cookies the most, and are also the ones who „accept without reading" the least
use social media and networking less frequently	use social media and the web more frequently

Source: based on the authors' own research.

26 Refusal of cookies – transmit other data: χ^2 (6, N = 518) = 23.215, p = .001. Refusal of cookies - read privacy policy: χ^2 (6, N = 518) = 36.030, p = .000. Refusal of cookies – restrict location access: χ^2 (6, N = 518) = 32,990, p = .000. Refuse cookies - restrict profile access: χ^2 (6, N = 512) = 22,501, p = .001. Refuse cookies – refuse public use consent: χ^2 (6, N = 518) = 80,329, p = .000. Cookie refusal – verify site security: χ^2 (6, N = 518) = 25,955, p = .000. Refuse cookies – request data access: χ^2 (6, N = 518) = 21,517, p = .001. Cookie refusal – block browser cookies: χ^2 (6, N = 518) = 66,311, p = .000.

From the contrasting observation of these two contradictory groups, we came up with the idea that perhaps the fact of having high (or low) values in these indices depended more on the frequency of network use than on opinions and differences between people. In other words, we decided to test the hypothesis that the rate of activity on the net was able to explain the variation in these indices more than the other variables taken into consideration so far and thus lead to the paradoxical condition that a high „net use" led the respondents to have, at the same time, a high „rate of defensive" and „non-defensive actions" (and vice versa). This hypothesis turned out to be false. The index of „non-defensive" actions is indeed directly and significantly correlated with the overall „network activity" rate (as one increases, so does the other)[27]. The correlation between the „defensive" and „activity index", on the other hand, is not significant. In addition to this, the correlation test applied to the two „defensive" and „non-defensive" indices indicates a (albeit weak) significant correlation between them, which is an inverse correlation[28], thus negating the hypothesis we described above.

Conclusion

To summarise, the data analysed so far tell us that the „awareness" of data transfer that occurs every time one uses the network is stated by all respondents and, therefore, seems to be shared. When one moves from the „awareness" of the data transfer to assessing the specific „concern" about this phenomenon, the leap backwards in the data is rather strong: apart from 5,6% of the respondents who indicate that they are „not at all concerned" about this, about half of the sample declares only slight concern (almost all of them give the nuanced answer „quite a lot" or „a little"). Only less than one in ten respondents declare themselves to be „very concerned".

On the other hand, the risk related to privacy is, for substantially all respondents, a risk related only to the commercial sphere and advertisements, while hints of more severe dangers are substantially absent. Moreover, observing the perception of risk with respect to devices and activities on the network and cross-referencing this data with those related to usage practices

27 Index of „non-defensive" actions – activity rate: $\tau_b = .310$, $p<.01$ (N = 518).
28 Index of „defensive" actions – index of „non-defensive" actions: $\tau_b = -.157$, $p<.01$ (N = 518).

and activities carried out, it can be seen that respondents tend to do and use precisely the actions and devices they indicate as the riskiest (thus implicitly denying the relevance of the risk itself, which they perceive that, given their behaviour, cannot really be high).

Thus, a high declared awareness level concerning data transfer is contrasted by a rather low specific concern. Concern that, in any case, is not sufficient to actually influence the behaviour of respondents on the Internet. If we add to this the fact that the device most commonly used (the smartphone) is the one that leads most to the transfer of multiple types of data and that is least configurable in respect of privacy protection[29], then the picture that emerges is, beyond words, a picture of a sample:

– only theoretically aware and unconcerned about privacy risks;
– which are underestimated and downplayed only to their commercial and visible aspects[30];
– where there is a large gap between the declared awareness of the risk and the behaviour implemented;
– as the behaviours indicated as the riskiest are also the most frequent behaviours.

As a result, although there is significant (in theory) awareness of cybersecurity threats among students at the University of Udine, their practical behaviours do not align with the desired ones that would protect them from these threats. This indicates the need for continuous education in this sphere throughout society, as students, being a group raised with technology, should also exhibit secure behaviours. If this is not the case, it is highly likely that older respondent groups will not adopt such behaviours when using technology[31]. It would be interesting to

29 Cookies on sites can sometimes be actively rejected; most applications, much used by respondents, on the contrary require overall prior approval that cannot be configured, except to a very small extent.

30 It appears that respondents are only aware of the actuality of data transfer in aspects evident in their perceived reality, such as the appearance of an advertisement in social media following exposure to certain content, and do not contemplate the possibility of greater risks.

31 Indeed, studies carried out with similar methodologies by the University of Udine, show that 1) digital competence is significantly low in the elderly age group of the population (compared with the data of the students presented here) and that; 2) awareness of cyber risks is equally low (significantly lower than the awareness declared by these students). A circumstance that in the elderly population often leads to a rejection of the use of digital tools instead of stimulating appropriate protective behaviour. See in this regard C. Melchior, *Gli anziani e lo scarso utilizzo (e desiderio) di tecnologia digitale*, „Salute e Società" 2023, vol. 1, no. 3, p. 106–120; idem, *Elderly People and the Barriers to Digital Education*, „Italian Journal of Sociology of Education" 2023, vol. 15, no. 2, p. 37–53.

replicate these studies in the future among Polish students and develop a shared model for technological education across European societies.

Bibliography

Adamczyk M., Karpiuk M., Soler U., *The use of new technologies in education – opportunities, risks and challenges in the times of intensive intercultural change*, „Edukacja Międzykulturowa" 2023, no. 4.

Angwin J., *Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance*, New York 2014.

Bencsik A., Karpiuk M., *Cybersecurity in Hungary and Poland. Military aspects*, „Cybersecurity and Law" 2023, no. 1.

Bencsik A., Karpiuk M., *The legal status of the cyberarmy in Hungary and Poland. An overview*, „Cybersecurity and Law" 2023, no. 2.

Boyd D., *It's Complicated: The Social Lives of Networked Teens*, Yale 2014.

Chałubińska-Jentkiewicz K., *Cyberodpowiedzialność. Wstęp do prawa cyberbezpieczeństwa*, Toruń 2023.

Czuryk M., *Cybersecurity as a premise to introduce a state of exception*, „Cybersecurity and Law" 2021, no. 2.

Czuryk M., *Restrictions on the Exercising of Human and Civil Rights and Freedoms Due to Cybersecurity Issues*, „Studia Iuridica Lublinensia" 2022, no. 3.

Czuryk M., *Supporting the development of telecommunications services and networks through local and regional government bodies, and cybersecurity*, „Cybersecurity and Law" 2019, no. 2.

Ejdys J., Soler U., *The society's attitude toward 5G technologies – a case study of Poland*, „Technological and Economic Development of Economy" 2023, vol. 29, no. 5.

Ferguson N., Schneier B., Kohno T., *Cryptography Engineering*, 2010.

General Data Protection Regulation, https://uodo.gov.pl/404 [access: 28.12.2023].

Hoffman I., Karpiuk M., *The local self-government's place in the cybersecurity domain. Examples of Poland and Hungary*, „Cybersecurity and Law" 2021, no. 1.

Karpiuk M., *Crisis management vs cyber threats*, „Sicurezza, Terrorismo e Societa" 2022, no. 2.

Karpiuk M., *Cybersecurity as an element in the planning activities of public administration*, „Cybersecurity and Law" 2021, no. 1.

Karpiuk M., *Tasks of the Minister of National Defence in the area of cybersecurity*, „Cybersecurity and Law" 2022, no. 1.

Karpiuk M., *The Local Government's Position in the Polish Cybersecurity System*, „Lex Localis – Journal of Local Self-Government" 2021, no. 3.

Karpiuk M., *The obligations of public entities within the national cybersecurity system*, „Cybersecurity and Law" 2020, no. 2.

Karpiuk M., A. Makuch, Soler U., *The role of the Cybersecurity Strategy of the Republic of Poland in ensuring cybersecurity*, „Polish Political Science Yearbook" 2023, vol. 52, no. 3.

Melchior C., *Gli anziani e lo scarso utilizzo (e desiderio) di tecnologia digitale*, „Salute e Società" 2023, vol. 1, no. 3.

Melchior C. *Elderly People and the Barriers to Digital Education*, „Italian Journal of Sociology of Education" 2023, vol. 15, no. 2.

Melchior C., *News and climate change: Opinions, degree of information and awareness of Italian university students* [in:] *Communities, technology and this moment*, eds. L. Stillman, M. Anwar, C. Rhinesmith, Melbourn 2021.

Mitnick K., *The Art of Deception: Controlling the Human Element of Security*, New Yersey 2002.

Mitnick K., Simon W. L., *Ghost in the Wires: My Adventures as the World's Most Wanted Hacker*, Boston 2011.

Mitnick K., Simon W. L., *The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders, and Deceivers*, New Jersey 2005.
Mitnick K., Vamosi R., *The Art of Invisibility*, Boston 2017.
Network and Information Security Directive, https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new [access: 28.12.2023].
Network and Information Security Directive 2, https://eur-lex.europa.eu/eli/dir/2022/2555 [access: 28.12.2023].
Noble S., *Algorithms of oppression: how search engines reinforce racism*, New York 2018.
Snowden E., *Permanent Record*, Macmillan, New York 2019.
Schneier B., *Applied Cryptography*, New Jersey 1996.
Schneier B., *Beyond Fear: Thinking Sensibly about Security in an Uncertain World*, New York 2003.
Schneier B., *E-Mail Security*, New Jersey 1995.
Schneier B., *Liars and Outliers: Enabling the Trust that Society Needs to Thrive*, New Jersey 2012.
Schneier B., *Protect Your Macintosh*, Berkley 1994.
Schneier B., *Secrets and Lies*, New Jersey 2000.
Schneier B., *Schneier on Security*, New Jersey 2008.
Schneier B., Banisar D., *The Electronic Privacy Papers*, New Jersey 1997.
Schneier B., Kelsey J., Whiting D., Wagner D., Hall C., Ferguson N., *The Twofish Encryption Algorithm*, New Jersey 1996.
Soler U., *Social perception of 5G technology*, „Rocznik Instytutu Europy Środkowej" 2022, R. 20, z. 1.
Soler U., *Technologia jako narzędzie wzmacniania więzi społecznych*, „Zeszyty Naukowe Politechniki Śląskiej". Ser. „Organizacja i Zarządzanie" 2028, t. 113.
Soler U., *The Role of Network Technologies in European Cybersecurity* [in:] *The Role of Cybersecurity in the Public Sphere – The European Dimension*, eds. K. Chałubińska-Jentkiewicz, I. Hoffman, Maribor 2022.
Soler U., Busiło M., *Oswajanie z technologią. Na przykładzie elektryfikacji Wielkiej Brytanii i technologii 5G*, „Przegląd Elektrotechniczny" 2019, R. 95, nr 12.
Soler U., Busiło M., *Education of society as a tool to counteract disinformation in implementing new technologies. On the example of 5G mobile telecommunications network and Warsaw sewage system* [in:] *Proceedings of the International Conference „Applications of Electromagnetics in Modern Engineering and Medicine" June 9–12, 2019, Janów Podlaski, Poland*, New York 2019.
Solve D., *Nothing to Hide: The False Tradeoff Between Privacy and Security*, Yale 2011.
The Privacy Issue. Decoding the Privacy Paradox, 2021, https://theprivacyissue.com/privacy-and-society/decoding-privacy-paradox [access: 28.12.2023].
Tufekci Z., *Twitter and tear gas: the power and fragility of networked protest*, New Haven 2017.
Zuboff S., *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, New York 2019.

Bezpieczeństwo danych osobowych w cyberprzestrzeni w opinii studentów uniwersytetu w Udine

Streszczenie

Wzrost obaw dotyczących bezpieczeństwa danych osobowych w cyberprzestrzeni wymaga wszechstronnego zbadania świadomości użytkowników, ich postaw i zachowań. Przeprowadzone wśród studentów uniwersytetu w Udine badanie skupiało się na wielu aspektach bezpieczeństwa danych osobowych, bada percepcję i zachowania związane z prywatnością, bezpieczeństwem sieciowym i zgodnością z przepisami prawnymi. Celem

badania była ocena świadomości respondentów transferu danych w sieci, ogólnych obaw związanych z ryzykiem cybernetycznym oraz związku między świadomością, obawami a rzeczywistymi zachowaniami online. Próba badawcza licząca 518 respondentów, głównie młodych osób, została zebrana za pomocą kwestionariusza online. Wyniki pokazały znaczącą rozbieżność między deklarowaną świadomością a rzeczywistymi obawami, prowadzą do „paradoksu prywatności". Respondenci wykazali świadomość transferu danych, ale ich konkretne obawy były ograniczone, skupiały się głównie na aspektach komercyjnych, zamiast uwzględniać szersze zagrożenia cyberbezpieczeństwa. Ta niezgodność dotyczyła również zachowań online i dominującego używania urządzeń takich jak smartfony, które jednocześnie są najczęściej używane przez respondentów, ale są również postrzegane jako najbardziej narażone na utratę danych i mają najmniejsze możliwości wdrożenia działań ochrony danych. Wyniki pokazały krytyczną potrzebę ciągłej edukacji z dziedziny cyberbezpieczeństwa, szczególnie skierowanej do młodych ludzi, żeby zmniejszyć różnicę między teoretyczną świadomością a praktycznym stosowaniem bezpiecznych praktyk online. Wyniki te sugerują potrzebę prowadzenia dalszych badań nad różnymi kontekstach kulturowymi i zaproponowanie wspólnego modelu edukacji technologicznej dla społeczeństw europejskich w celu promowania bezpiecznych zachowań w cyfrowym świecie.

Słowa kluczowe: dane osobowe, bezpieczeństwo, cyberbezpieczeństwo, „paradoks prywatności", badania socjologiczne, edukacja technologiczna