PRO PUBLICO BONO – Public Administration, 2021/4, 124–141. • DOI: 10.32575/ppb.2021.4.8

Vivien Kardos

PRIVACY LITERACY AND THE PROTECTION OF PERSONAL DATA IN THE MIND OF LAW STUDENTS

Vivien Kardos, PhD student, University of Szeged, Faculty of Law and Political Sciences, Department of Statistics and Demography, kardos.vivien.kata@gmail.com

With the advent of the fourth industrial revolution, the issue of data protection has become more important than ever before. There is no doubt that data, and especially personal data, has significant commercial value. Data protection also raises major issues for the legal profession. With the increasing significance of data protection, the question arises as to whether law students have sufficient knowledge of privacy literacy.

Based on the results of empirical research, this study set out to examine the attitudes of current law students to personal data and to determine how seriously they take data protection, particularly how it works in practice, when, for example, they use various kinds of social network sites, as well as to gauge their knowledge of data protection guarantees. The aim of this study is to provide a brief insight, based on the results of in-depth interviews, into the reasons behind the specific privacy literacy gaps revealed by the findings of the preliminary quantitative research.

It is anticipated, it should be emphasised, that law students will prove not to be fully aware of how much personal data they may provide about themselves on social network sites. Moreover, identifying personal data through practical examples causes difficulties for law students, such as cookie ID or data on their health. Consequently, the privacy literacy of law students needs to be improved.

Keywords:
cookies, data protection, data protection guarantees, empirical research, GDPR, personal data breach

1. INTRODUCTION

According to the latest edition of *Internet World Stats,* there are approximately 4.93 billion Internet users worldwide.[1] The use of social media platforms has long been an ordinary part of the lives of 'digital natives'.[2] According to Article 4 (1) of Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, 'GDPR'), personal data means any information relating to an identified or identifiable natural person (a 'data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. It can be stated that this definition involves a lot of information about a natural person and has a broad interpretation, which is why it is important to identify personal data in any situation.

In this context, it seemed pertinent to investigate how the perception of personal data develops among a specific subject group, in this case law students, who may thus also increase their knowledge of data protection. The first question is what their viewpoint is about the importance of their personal data and how this is reflected in practice when using, for example, different kinds of social media platforms. Can it be clearly established that they can identify personal data properly, or do difficulties arise due to a lack of knowledge of the broad interpretation of personal data? Before continuing, I will outline why I opted to examine the perspective of law students on personal data and what their attitude is to data protection and privacy in the world of social media sites.

One reason for this focus is that these individuals will go on to be the lawyers of the future even though they are still at university at present. It is difficult to imagine that they will not encounter some aspects of data protection in their work, thus it is particularly important that they focus on improving their privacy literacy beforehand. Furthermore, it is assumed that their knowledge related to data protection has been enhanced during their university years. In support of this assumption, it may be established through the responses of law students that they have dealt with data protection at different depths in various kinds of courses. The aim of this study is to provide a brief insight, based on the results of in-depth interviews, into the reasons behind certain privacy literacy gaps, which can be ascertained from the findings of the preliminary quantitative research ('preliminary research' or 'questionnaire') performed by the author. It will also highlight some of the significant issues in connection with the privacy literacy of the law students.[3]

---

1 Internet World Stats, *World Internet Usage and Population Statistics* (2020 Q3 Estimates, 30 September 2020). World total Internet users: 4,929,926,187.

2 Marc Prensky, 'Digital Natives, Digital Immigrants', *On the Horizon* 9, no 5 (2001).

3 Vivien Kardos, 'Insight into the perception of personal data among law students', in *Central and Eastern European e|Dem and e|Gov Days 2020 – Conference Proceedings,* ed. by Thomas Hemker, Robert Müller-Török, Alexander Prosser, Dona Scola, Tamás Szádeczky and Nicolae Urs (Facultas, Austrian Computer Society, 2020), 126.

2. LITERATURE REVIEW

Literacy can be defined by the fusion of two types of competence: knowledge and skills.[4] The concept of digital literacy may seem to be nearly synonymous with privacy literacy these days, although it should be emphasised that there are significant differences between the two terms. The term privacy literacy refers to an understanding of the responsibilities and risks associated with sharing information online, while digital literacy focuses on the task-based use of information in a digital environment.[5]

Privacy literacy is "the understanding that consumers have of the information landscape with which they interact and their responsibilities within that landscape".[6] It is commonly argued that people with higher levels of knowledge of data protection, including the theoretical "know it" and the practical "know how" knowledge, tend to protect their privacy better. Privacy literacy is a combination of such knowledge and actual practice, as it includes both elements.[7] From the point of view of developing the data protection of students, privacy literacy has many useful aspects, for instance it is a good basis for strengthening online privacy.[8] Research has highlighted the users' lack of knowledge of privacy and of the skills to protect it.[9]

"Online privacy literacy within the frame of digital literacy is thus crucial for users' knowledge and awareness increase as well as skills enhancement in order for them to be able to assess risks resulting from information disclosure, adopt technical mechanisms and strategies for combating cyber threats and, consequently, protect themselves efficiently".[10] According to Givens, the definition of privacy literacy can be established as "one's level of understanding and awareness of how information is tracked and used in online environments and how that information can retain or lose its private nature".[11] The question could be raised as to precisely which skills are included in terms of privacy literacy. At present there is no widely-accepted list of the privacy literacy skills which constitute privacy literacy.[12]

---

4 Maria Sideri et al., 'Enhancing university students' privacy literacy through an educational intervention: a Greek case-study', *International Journal of Electronic Governance* 11, nos 3–4 (2019), 336.

5 Christina L Wissinger, 'Privacy Literacy: From Theory to Practice', *Communications in Information Literacy* 11, no 2 (2017), 379.

6 Jeff Langenderfer and Anthony D Miyazaki, 'Privacy in the Information Economy', *The Journal of Consumer Affairs* 43, no 3 (2009), 380–388.

7 Sabine Trepte et al., 'Do People Know about Privacy and Data Protection Strategies? Towards the 'Online Privacy Literacy Scale' (OPLIS), in *Reforming European Data Protection Law,* ed. by Serge Gutwirth, Ronald Leenes and Paul de Hert (Heidelberg: Springer, 2015), 343.

8 Miriam Bartsch and Tobias Dienlin, 'Control your Facebook: An analysis of online privacy literacy', *Computers in Human Behavior* 56 (2016), 149.

9 Yong J Park, 'Digital Literacy and Privacy Behavior Online', *Communication Research* 40, no 2 (2011), 215–236.

10 Sideri et al., 'Enhancing university students' privacy literacy', 336.

11 Cherie L Givens, *Information Privacy Fundamentals for Librarians and Information Professionals* (New York: Rowman and Littlefield, 2015).

12 Wissinger, 'Privacy Literacy: From Theory to Practice', 380.

As Szőke stated in his study, the different generations of the regulation of data protection try to respond to the societal changes driven by the current technological revolutions.[13] Furthermore, according to Baek, digital literacy appears to have a positive impact on the protection of online privacy,[14] while its level is related to an understanding of technical terms such as "cookies", behaviourally targeted advertising and data mining.[15] In the context of the usage of social networking sites, studies show that technical knowledge, skills and the knowledge of privacy settings is positively correlated with alteration of privacy settings.[16] The study of Vladlena Benson et al. also confirms the positive relationship between user awareness and lower levels of disclosure of information.[17]

Use of social media often does not provide alarms that might remind people to be aware of their privacy; in addition, digital environments that seem to be private can often become completely public without any significant effort and forewarning.[18]

As has been noted in the literature "knowledge provides decision making control[19] and affects individuals' behaviour[20] which could be thought to include information sharing in online social networks".[21]

According to Calin Veghes et al. privacy literacy can be seen as a new concept "proposed in order to assess and explain the consumers' attitude regarding the collection, processing and employment of their personal data" in the context of direct marketing.[22]

---

13 Gergely L Szőke, 'Az adatvédelem szabályozásának történeti áttekintése', *Infokommunikáció és Jog* 56, no 3 (2013), 111.

14 Young M Baek et al., 'My privacy is okay, but theirs is endangered: Why comparative optimism matters in online privacy concerns', *Computers in Human Behavior* 31, no 1 (2014), 48–56; Park, 'Digital Literacy', 220.

15 Eszter Hargittai, 'An update on survey measures of web-oriented digital literacy', *Social Science Computer Review* 27, no 1 (2009), 133; Park, 'Digital Literacy', 227.

16 Danah Boyd and Eszter Hargittai, 'Facebook privacy settings: Who cares?', *First Monday* 15, 8 (2010); Murat Kezer et al., 'Age differences in privacy attitudes, literacy and privacy management on Facebook', *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 10, no 1 (2016).

17 Vladlena Benson et al., 'Information disclosure of social media users: Does control over personal information, user awareness and security notices matter?', *Information Technology & People* 28 no 3 (2015), 429.

18 Kate Raynes-Goldie and Matthew Allen, 'Gaming Privacy: A Canadian Case Study of a Co-Created Privacy Literacy Game for Children', *Surveillance and Society* 12, 3 (2014), 415.

19 Icek Ajzen and B L Driver, 'Prediction of Leisure Participation from Behavioral, Normative, and Control Beliefs: An Application of the Theory of Planned Behavior', *Leisure Sciences* 13, no 3 (1991), 185–204; Christopher J Armitage and Mark Conner, 'The Theory of Planned Behavior: Assessment of Predictive Validity and Perceived Control', *British Journal of Social Psychology* 38, no 1 (1999), 35–54; Naveen F Awad and M S Krishnan, 'The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to be Profiled Online for Personalization', *MIS Quarterly* 30, no 1 (2006), 13–28; Tanya L Chartrand, 'The Role of Conscious Awareness in Consumer Behavior', *Journal of Consumer Psychology* 15, no 3 (2005), 203–210.

20 Tom Buchanan et al., 'Development of Measures of Online Privacy Concern and Protection for Use on the Internet', *Journal of the American Society for Information Science and Technology* 58, no 2 (2007), 157–165.

21 Bobbi Morrison, 'Do we know what we think we know? An exploration of online social network users' privacy literacy'. *Proceedings of the 42nd Atlantic Schools of Business Conference,* Dalhousie University, 2012, 420–421.

22 Călin Vegheş et al., 'Privacy Literacy: What is and how it can be measured', *Annales Universitatis Apulensis Series Oeconomica* 14, no 2 (2012), 705.

Given the importance of expressing consent, at present "privacy as control" theories prioritise the role of choice and individual self-determination over other values. As such, it should be noted that they can be described as information management theories, where this kind of control is achieved through the subjective management and expression of personal preferences.[23]

A case study[24] by Maria Sideri et al. investigated the privacy literacy of university students in relation to the usage of social media. To this end, they held a thirteen-week course on social media, attended by 54 students, 23 of whom volunteered to take part in the research. During the course, students learnt how to isolate their profiles from undesirable audiences, and the goal of strengthening privacy literacy was achieved through the educational intervention. Although the students confirmed that they have a responsibility to protect themselves and others on their chosen social media platform (Facebook), the results of the research revealed that, at the outset, they did not have the necessary knowledge in this field. Nevertheless, after completing the course, many of the participants exercised more caution with regard to their profile visibility and also paid more attention to the privacy settings of Facebook, while their uncertainty awareness of the usefulness of anti-spyware software increased.[25] This research shows the important role that education can play in developing privacy literacy, which is intimately connected to privacy awareness.

Murat Kezer et al. examined the privacy behaviours of American adults on Facebook in their study. Based on life-cycle theory, it compares social media users from three age groups – young adults (18–40 years), middle-aged adults (40–65 years) and mature adults (over 65 years) – in terms of their knowledge of and attitudes towards data protection and privacy concerns, as well as the impact of these factors on self-disclosure and their privacy behaviour on Facebook.[26] No significant difference was found between the age groups' belief in the right to data protection and their degree of concern about their own data protection. In contrast, they paid attention to the extent of their own data protection more actively than focusing on how the personal data of other people around them were protected. In particular, the group of mature adults mostly believed that the protection of their own personal data depends on whether the people around them protect it. Young adults are less likely to appreciate the protection of personal data of others.[27] It should be highlighted that this finding is also consistent with the results of the present research.

---

23 Daniel J Solove, 'Privacy Self-Management and the Consent Paradox', *Harvard Law Review* 126, no 7 (2013), 1880–1903; Christophe Lazaro and Daniel Le Métayer, 'Control over Personal Data: True Remedy or Fairy Tale?', *Scripted* 12, no 1 (2015), 7.

24 Sideri et al., 'Enhancing university students' privacy literacy', 342.

25 Ibid. 353.

26 Kezer et al., 'Age differences'.

27 Ibid. 7.

3. BACKGROUND – THE PRELIMINARY RESEARCH

3.1. Method

Before presenting the research on which this study is based, it is important to highlight the factors that have contributed to it and affected the conduct of the research. The research was based on a questionnaire, which was carried out on a voluntary basis, conducted on an online interface, with the participation of a total of 205 law students from all eight faculties of law in Hungary. The distribution of women and men respondents in the research was 63 per cent and 37 per cent respectively. The majority of them were full-time students, in all years from the first to the final year of their course. Moreover, some correspondence students also took part in order to broaden the investigational spectrum. The data collection took place at the beginning of 2020. The questionnaire included questions on several fields of data protection and privacy literacy.

The questionnaire covered the topics of general data protection and the usage of social network sites ('SNSs'), with particular emphasis on the sharing and accessibility of personal data. Topics addressed included daily usage of SNSs, password protection of digital devices and personal data breaches. The key consideration in the creation of the questions was to their utility in measuring knowledge, attitudes and habits. To achieve realistic results, some questions were related to practical issues, such as what types of personal data the participants share on SNSs. The question format varied, with some requiring single responses and others multiple responses in the form of direct and indirect questions. Furthermore, scales of one to ten were also used in some items.

3.2. Main findings

Before going into a detailed analysis of the results, the main findings of the questionnaire can be determined as follows: Although the law students recognised the importance of data protection, their "activity" on SNSs is not fully in accordance with their statements. Approximately 95 per cent of the respondents use some form of SNSs on a daily basis. Not surprisingly, Facebook is the most common, although nearly three quarters of the respondents had not read the privacy policy at all. This was also reflected in their attitudes.

One of the most remarkable results of the preliminary research is that it can be established that the law students surveyed had difficulty identifying personal data through practical examples. For example, only a total of 27 per cent of the law students classified cookie identifiers ('cookie ID') correctly as personal data. A significant difference was found between the responses of male and female respondents, with approximately 39 per cent of the men giving the correct response, while 20 per cent of women chose another option. When asked about the IP address of one's laptop, about 60 per cent of the respondents answered correctly, with almost the same proportion of men and women. Cell phone

location data was classified as personal data by 80 per cent of the law students, with quite similar proportions for both men and women. In contrast, when the question related to the advertising ID of the mobile phone, it was quite difficult to decide whether it is personal data or not, as 38 per cent of the respondents responded correctly, and again the proportion of men and women was almost the same. On data concerning health, the diagnosis on an outpatient information sheet was correctly classified as personal data by approximately 93 per cent of the respondents (almost the same proportion of men and women). Conversely, when asked about an X-ray of a broken tibia a total of about 79 per cent of the respondents gave the correct response, 81 per cent of women and 76 per cent of men.

These results underline the lack of knowledge of the surveyed students in relation to the identification of personal data through practical examples. In this context, there were significant gaps in the respondents' knowledge of the privacy aspects of data concerning health, as well as the status of cookie IDs and the issue of mobile (cell) phones. This led us to ask the law students additional questions in order to shed light on the underlying causes of this lack of awareness.

Knowledge gaps were also revealed in connection with the cookie ID, which will be presented in detail later, given that the highest error rate was related to this kind of personal data, and contradictory results were obtained. Briefly, most of the law students basically do not know what exactly a cookie ID means. Furthermore, approximately three quarters of the law students asserted that they were unaware of data protection guarantees.

4. IN-DEPTH INTERVIEWS – THE QUALITATIVE RESEARCH

4.1. Method

In order to identify the underlying causes of the level of awareness and to achieve a broader scope of research, 16 in-depth interviews were conducted with two law students from each of the faculties of law[28] in Hungary. The interviews were conducted with the consent of the interviewees, who participated voluntarily, and the information was used anonymously. The interviews were conducted with the aid of a telecommunication tool, and the interviews lasted an average of 18 minutes.

The age of the interviewees, who were in various years of the university courses, ranged from 21 to 29 years, with an average age of 22.81 years. The gender distribution can more or less be considered as balanced, since nine men and seven women were interviewed. The questions focused on assessing the privacy practices, attitudes and knowledge of law students in the light of the gaps in knowledge identified above.

[28] Eötvös Loránd University, Faculty of Law; Károli Gáspár University of the Reformed Church in Hungary, Faculty of Law; Pázmány Péter Catholic University, Faculty of Law and Political Sciences; University of Debrecen, Faculty of Law; University of Győr, Deák Ferenc Faculty of Law; University of Miskolc, Faculty of Law; University of Pécs, Faculty of Law; University of Szeged, Faculty of Law and Political Sciences.

4.2. Results

Before analysing the in-depth interviews, it should be noted that the vast majority of the respondents had already heard about certain aspects of data protection in their university courses. In this regard, the differences in the depth of this type of knowledge varied between the students according to how much they were able to tangentially gain knowledge or experiences of it from various courses taken in semesters over a number of years. The courses dealing with data protection which the respondents mentioned included, but were not limited to, constitutional law, info-communication and media law, legal informatics, civil law and labour law. Moreover, one student reported that she had attended an optional course specifically on data protection.

Additionally, all of the respondents stated that they had already encountered data protection beyond the university walls in several situations. Examples included writing research papers on the subject of data protection, dealing with data protection matter during internships in law firms, participation in a briefing at the National Authority for Data Protection and Freedom of Information ('the NAIH') or even approving the data processing policies, other briefings and regulations on social media platforms. All of the interviewees use Facebook and 13 of them also use Instagram daily. Furthermore, LinkedIn, Snapchat and Reddit were also mentioned on occasion.

4.2.1. 'Is it personal data?'

Based on the results of the preliminary research, it became evident that using practical examples to identify personal data had posed difficulties for the students who were surveyed, particularly cookie IDs and data concerning health,[29] thus eleven pieces of information were presented during the interview. The examples of information and personal data used were: a cookie ID; a medical prescription that must be purchased at a pharmacy; the advertising ID of one's mobile phone; the IP address of one's laptop; cell phone location data; an X-ray of 'your' broken tibia; a sonogram of your internal organs; the company registration number of the commercial service company in 'your' place of residence; the ID number on the residence card; 'your' own address and a diagnosis on an outpatient information sheet. Most of these had already been mentioned in the preliminary research.

In line with results of the questionnaire, the personal data nature of one's address and the medical diagnosis on the information sheet were obvious for approximately 93 per cent of the respondents. It should also be noted that there were no examples of all of the law students knowing the correct answer. This is also thought-provoking, because these were the easiest questions. However, respondents had less success identifying 'untypical' types

[29] Art. 4. (15) GDPR. Data concerning health means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

of personal data, for instance cookie ID or the IP address of the laptop, not to mention the advertising ID of the mobile phone or cell phone location data. As such, the majority of the law students selected and stated the wrong response to questions related to these items.

It became apparent that the identification of personal data is a real challenge for law students, when they had to identify 'atypical' examples of personal data. Interviewees gave different responses to questions about similar data concerning health, thereby confirming the uncertainty of their knowledge in connection with personal data. All of the interviewees knew that the diagnosis on an outpatient information sheet is personal data, but only three of them gave a correct answer in connection with a medical prescription which must be purchased at a pharmacy. In addition, ten interviewees said that X-rays and sonograms were also personal data. The students' responses to these questions revealed that they did not have knowledge of these examples of personal data, particularly when the data concerned health. A significant difference could be established – over 13 per cent – between determining the legal nature of X-rays and the diagnosis on the outpatient information sheet.

Confirming the results of the preliminary research, it can be established that the most difficult type of personal data to identify for the respondents was the cookie ID, with the majority of students' believing that cookies are not personal data. However, this is a mistaken statement. Summarising the identification of personal data by the two types of methodology, almost the same results can be seen.

4.2.2. 'The most personal data' which is shared

The respondents were asked a separate question: which data they considered to be the most personal type of data. Another question concerned the attitude of the law students to 'the most personal data' that they still share or would share on social media platforms as well as information that is so personal that they do not share it at all. The responses to these questions were quite varied and showed significant differences.

The interviewees closely associated telephone numbers and email addresses with privacy, as the vast majority of them do not share these on social media platforms, although one of the interviewees said that he/she shares both with his/her friends. Most of the interviewees stated that they share their date of birth and the university they attend on these platforms. One of the interviewees stated that she would not share her educational background. The responses indicated that most of the interviewees share their place of residence, but not the exact address. Notably, three students said that they do not share their exact current location, for instance if they are on holiday abroad, because they are afraid of a burglary. It should be emphasised that this practice shows both knowledge and appropriate action, as in this case the action is not sharing personal data. From the point of view of data protection, it is certainly questionable that one of the interviewees would

even share their identity card number on SNSs. In contrast, the other interviewees stated that they had not shared any personal documents or card details on social media at all.

This question highlighted what significant differences can be established between respondents with regard to the sharing of personal data. This suggests that some students may not be aware of the possible risks and consequences of such actions and therefore share a lot of personal data about themselves.

4.2.3. The issue of 'cookies'

The question could be raised as to why this issue is so important. The questionnaire showed that law students have an incomplete knowledge of this area of personal data, and conceptual disorders can also be identified. This topic is also significant from the perspective of knowledge and attitude. The cookie ID has an extremely close relationship with data protection and law students are likely to encounter many examples of it every day, which is why it was given a prominent role in the preliminary research.

One of the main findings was that law students often encounter pop-up 'cookie-windows' in everyday life and most of them were able to determine the meaning of them by choosing the right response from the alternatives. Notwithstanding this, there are significant shortcomings in the students' evaluation of their operation and legal nature. Even so, 87 per cent of the respondents indicated the correct answer from the six alternatives to define its meaning. In this context, it should be emphasised that barely more than a quarter of law students classified a cookie ID as personal data. Nevertheless, two thirds of the law students considered it 'risky' from a data protection point of view.

The results prompted me to ask further questions to explore where this uncertainty of knowledge could have originated from. The first question in this respect asked interviewees whether they would accept cookie policies and allow cookies. With the exception of two respondents, all interviewees would accept them, but significant differences can be established between the underlying reasons.

One of the two negative responses were for inherent privacy or data protection reasons and the other one was out of convenience, as the interviewee stated that they did not consider it important, as it was just slowing down the sites. The other answers were basically about streamlining the browsing experience. Furthermore, the respondents mentioned that articles cannot be read, or the person is not able to move on to the websites without accepting cookies. Four of them indicated that they were otherwise aware of the consequences. One interviewee pointed out that he deletes all cookies monthly, while others minimised the placement of cookies in settings. It is also decisive for attitudes that one student admitted that he was not aware of what he was accepting, and two interviewees stated that it was an inappropriate behaviour and habit, moreover, irresponsible to accept cookies without consideration. Against this background, it can be concluded that the majority of the law students have given their consent without being aware of the fact that their browsing habits can be followed in this way.

Subsequently, it was asked what cookies meant. Reflecting on the high rate of correct responses in the preliminary research, it can be seen that inference played a more important role than real knowledge, as, when no response alternatives were available, only three interviewees were able to give a relatively satisfactory response. Eleven interviewees explicitly stated that they had not known what it was, nor had they attempted to circumscribe the definition of it.

Nearly 70 per cent of the law students indicated that they considered cookies to be 'risky' from the point of view of privacy. Therefore, interviewees were asked whether they had concerns about privacy in connection with cookies and asked to outline their way of reasoning. This open-ended question provided an opportunity to visualise, in the light of the reasoning, how broad the spectrum of the interviewees' opinions is. Seven interviewees responded that they had already thought about privacy concerns in the context of cookies, while four of them mentioned personalised marketing as an example. Two interviewees' points of view were explicitly positive about the convenience feature of the cookies. Three law students said that this topic was neutral, because they had no negative experience of the utilisation of their personal data. Two respondents inferred from the question that they probably have, although they also noted that they had never been interested in this topic enough to seek further information. Differences in attitudes were also evident in this case, as, contrary to the previous responses, one interviewee admitted that he had not possessed the knowledge, but he considered that this was a huge mistake on his part and stated that he should have read up on this subject.

Another interviewee stated that he had discussed the topic with his friends because they had talked about it during a course on legal informatics. One of the answers drew attention to a specific potential privacy concern connected to visiting sites via a mobile phone when cookies have been accepted, in particular the way in which it is recorded, which also gives rise to a degree of intrusion into personal messages.

Confirming the results of preliminary research, it can be stated that many law students have a significant lack of knowledge regarding cookies. They give their consent without even knowing what exactly they are consenting to, and this could make efficient data protection difficult. Moreover, this attitude is also likely to manifest itself in other cases. This issue is not a new one, because according to *Conger* the students voluntarily provide this consent without any consideration to its collection, ignoring the fact that such information is currently not under their control, but under the control of the organisations that possess it.[30] Furthermore, many of them are not interested in what happens to this information.

[30] Sue Conger, Joanne H Pratt and Karen D Loch, 'Personal information privacy and emerging technologies', *Information Systems Journal* 23, no 5 (2013), 401–417.

4.2.4. Personal data breach

During the interviews, law students were asked whether they had already experienced a personal data breach and in general what their knowledge is about the meaning of such a breach. According to Article 4 (12) of the GDPR, a personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Based on the responses, it can be concluded that the vast majority of students were able to describe what the concept of personal data breach means. However, it should be noted that it was interpreted narrowly, which was shown by the examples. Only one student stated that it could happen accidentally, without bad faith. All the other respondents linked personal data breaches with unlawfulness. Four interviewees mentioned hacking of various user accounts as an example, and in seven cases, they identified it in general terms, for instance unauthorised use of personal data by a third party, misuse of personal data, unauthorised data transfer and unauthorised use of a telephone number. One interviewee admitted that he had not heard of this legal term at all, which also draws attention to the need to increase awareness of it, as on the one hand, the personal data breach has to be recognised before taking any further actions.

The main finding on this issue is that the concept of personal data breach needs to be interpreted in a much broader way. It can be established that most of the law students lack knowledge in this field. This issue is important because if a student does not have sufficient knowledge of what constitutes a personal data breach, then he or she will not be able to effectively deal with a potential breach, as it should be remembered that such breaches can happen accidentally.

4.2.5. Data protection guarantees

As the preliminary research demonstrated, the majority of the law students cannot give an example of or outline a data protection guarantee at all. This may also call into question the effectiveness of data protection. Hence, this issue can clearly be classified as one of the areas in which law students' knowledge needs to be extended as soon as possible. A separate question aimed to measure the knowledge and awareness of the law students, specifically to find out what kind of data protection guarantees they are aware of. The preliminary assumptions which they referred to were, for example, the principle of purpose limitation or the right to be forgotten. None of these were adequately expressed by the students and only two of the respondents stated the necessity of consent, and the acceptance of privacy policy statements.

Seven interviewees stated that they did not know, could not remember, or had not learnt about data protection guarantees in enough depth to remember it. Six students mentioned examples of European and national legislation in connection with this issue. It should be noted that one student referred only to an international treaty, thus presuming that

he is not familiar with either GDPR or domestic law, especially the Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information, although nowadays both are highlighted in many contexts. Although this may seem to be an isolated case, the respondent is probably not alone in this lack of knowledge, which is a significant finding. In addition, the NAIH was mentioned in two answers, although it should be noted that in both of them its full name was given incorrectly.

4.2.6. Changes in the content sharing habits

The interviews were extensively studied to identify potential changes in the content sharing habits of the law students. Basically, as the number of social media sites grows, the amount of personal data shared by users has constantly increased.[31] This finding can be confirmed in general.

Notwithstanding this trend, eleven interviewees stated that they share considerably fewer photos, posts and comments on social media platforms nowadays than they shared five years ago. Based on the responses, university life and age-related differences played a decisive role in these changes, and the preferences of the interviewees have also changed, as they claim to want to share less personal data. One respondent stated that the reason why she had shared less information and personal data is connected to her future job.

5. CONCLUSION

It can clearly be established that personal data is becoming more and more valuable in today's society. In order for data protection guarantees to prevail, it is essential for individuals also to pay attention to data protection in their daily lives. While all the interviewees in this study acknowledged the importance of data protection, considerable differences were found in their level of knowledge of privacy literacy. The responses to the questionnaire suggest that the identification of personal data through practical examples is difficult for law students.

The results of the research have shown that the level of privacy literacy needs to be improved in order to achieve a higher level of data protection with appropriate efficiency for law students. Extension of their existing knowledge and bridging the gaps in their privacy literacy is essential. Overall, based on the results of the study, it can be stated that law students have only superficial knowledge of many areas of data protection, they have difficulties with the issues related to it and the knowledge they do have has not been properly applied in practice.

[31] Christina L Wissinger and B Gail Wilson, 'Student Perceptions of Facebook's Privacy Policies and Rights', *Social Media Studies* 2, no 1 (2015), 15–26.

The 16 in-depth interviews, together with the preliminary research with the participation of 205 law students, are sufficient to establish patterns and raise further research questions, such as how well students are aware of the data protection risks and their possible consequences. In addition, less self-evident deficiencies in knowledge may also have emerged. Given that law students pay more attention to data protection than people in other fields, presumably due to the profession, it is likely that average university students reflect on this topic even less. In order to develop privacy literacy, it is necessary to teach practically-oriented knowledge to law students during their studies, so that future law professionals can go on to apply their knowledge properly in practice.

REFERENCES

1. Ajzen, Icek and B L Driver, 'Prediction of Leisure Participation from Behavioral, Normative, and Control Beliefs: An Application of the Theory of Planned Behavior'. *Leisure Sciences* 13, no 3 (1991), 185–204. Online: https://doi.org/10.1080/01490409109513137
2. Armitage, Christopher J and Mark Conner, 'The Theory of Planned Behavior: Assessment of Predictive Validity and Perceived Control'. *British Journal of Social Psychology* 38, no 1 (1999), 35–54. Online: https://doi.org/10.1348/014466699164022
3. Awad, Naveen F and M S Krishnan, 'The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to be Profiled Online for Personalization'. *MIS Quarterly* 30, no 1 (2006), 13–28. Online: https://doi.org/10.2307/25148715
4. Baek, Young M, Eun M Kim and Young Bae, 'My privacy is okay, but theirs is endangered: Why comparative optimism matters in online privacy concerns'. *Computers in Human Behavior* 31, no 1 (2014), 48–56. Online: https://doi.org/10.1016/j.chb.2013.10.010
5. Bartsch, Miriam and Tobias Dienlin, 'Control your Facebook: An analysis of online privacy literacy'. *Computers in Human Behavior* 56 (2016), 147–154. Online: https://doi.org/10.1016/j.chb.2015.11.022
6. Benson, Vladlena, George Saridakis and Hemamaali Tennakoon, 'Information disclosure of social media users: Does control over personal information, user awareness and security notices matter?' *Information Technology & People* 28, no 3 (2015), 426–441. Online: https://doi.org/10.1108/ITP-10-2014-0232
7. Boyd, Danah and Eszter Hargittai, 'Facebook privacy settings: Who cares?' *First Monday* 15, no 8 (2010). Online: https://doi.org/10.5210/fm.v15i8.3086
8. Buchanan, Tom, Carina Paine, Adam N Joinson and Ulf-Dietrich Reips, 'Development of Measures of Online Privacy Concern and Protection for Use on the Internet'. *Journal of the American Society for Information Science and Technology* 58, no 2 (2007), 157–165. Online: https://doi.org/10.1002/asi.20459
9. Chartrand, Tanya L, 'The Role of Conscious Awareness in Consumer Behavior'. *Journal of Consumer Psychology* 15, no 3 (2005), 203–210. Online: https://doi.org/10.1207/s15327663jcp1503_4
10. Conger, Sue, Joanne H Pratt and Karen D Loch, 'Personal information privacy and emerging technologies'. *Information Systems Journal* 23, no 5 (2013), 401–417. Online: https://doi.org/10.1111/j.1365-2575.2012.00402.x
11. Givens, Cherie L, *Information Privacy Fundamentals for Librarians and Information Professionals.* New York: Rowman and Littlefield, 2015.
12. Hargittai, Eszter, 'An update on survey measures of web-oriented digital literacy'. *Social Science Computer Review* 27, no 1 (2009), 130–137. Online: https://doi.org/10.1177/0894439308318213
13. Internet World Stats, *World Internet Usage and Population Statistics.* 2020 Q3 Estimates, 30 September 2020. Online: www.internetworldstats.com/stats.htm

14. Kardos, Vivien, 'Insight into the perception of personal data among law students', in *Central and Eastern European e|Dem and e|Gov Days 2020 – Conference Proceedings,* ed. by Thomas Hemker, Robert Müller-Török, Alexander Prosser, Dona Scola, Tamás Szádeczky and Nicolae Urs. Facultas, Austrian Computer Society, 2020, 125–134. Online: https://doi.org/10.24989/ocg.v.338.10
15. Kezer, Murat, Barış Sevi, Zeynep Cemalcilar and Lemi Baruh, 'Age differences in privacy attitudes, literacy and privacy management on Facebook'. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 10, no 1 (2016). Online: https://doi.org/10.5817/CP2016-1-2
16. Langenderfer, Jeff and Anthony D Miyazaki, 'Privacy in the Information Economy'. *The Journal of Consumer Affairs* 43, no 3 (2009), 380–388. Online: https://doi.org/10.1111/j.1745-6606.2009.01152.x
17. Lazaro, Christophe and Daniel Le Métayer, 'Control over Personal Data: True Remedy or Fairy Tale?' *Scripted* 12, 1 (2015), 1–25. Online: https://doi.org/10.2966/scrip.120115.3
18. Morrison, Bobbi, 'Do we know what we think we know? An exploration of online social network users' privacy literacy'. *Proceedings of the 42nd Atlantic Schools of Business Conference,* Dalhousie University, 2012.
19. Park, Yong J, 'Digital Literacy and Privacy Behavior Online'. *Communication Research* 40, no 2 (2011), 215–236. Online: https://doi.org/10.1177/0093650211418338
20. Prensky, Marc, 'Digital Natives, Digital Immigrants'. *On the Horizon* 9, no 5 (2001). Online: https://doi.org/10.1108/10748120110424816
21. Raynes-Goldie, Kate and Matthew Allen, 'Gaming Privacy: A Canadian Case Study of a Co-Created Privacy Literacy Game for Children'. *Surveillance and Society* 12, 3 (2014), 414–426. Online: https://doi.org/10.24908/ss.v12i3.4958
22. Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
23. Sideri, Maria, Angeliki Kitsiou, Eleni Tzortzaki, Christos Kalloniatis and Stefanos Gritzalis, 'Enhancing university students' privacy literacy through an educational intervention: a Greek case-study'. *International Journal of Electronic Governance* 11, nos 3–4 (2019), 333–360. Online: https://doi.org/10.1504/IJEG.2019.10018628
24. Solove, Daniel J, 'Privacy Self-Management and the Consent Paradox'. *Harvard Law Review* 126, no 7 (2013), 1880–1903.
25. Szőke, Gergely L, 'Az adatvédelem szabályozásának történeti áttekintése'. *Infokommunikáció és Jog* 56, no 3 (2013), 107–112.
26. Trepte, Sabine, Doris Teutsch, Philipp K Masur, Carolin Eicher, Mona Fischer, Alisa Hennhöfer and Fabienne Lind, 'Do People Know about Privacy and Data Protection Strategies? Towards the 'Online Privacy Literacy Scale' (OPLIS)', in *Reforming European Data Protection Law,* ed. by Serge Gutwirth, Ronald Leenes and Paul de Hert. Heidelberg: Springer, 2015, 333–365. Online: https://doi.org/10.1007/978-94-017-9385-8

27. Vegheş, Călin, Mihai Orzan, Carmen Acatrinei and Diana Dugulan, 'Privacy Literacy: What is and how it can be measured'. *Annales Unversitatis Apulensis Series Oeconomia* 14, no 2 (2012), 704–710. Online: https://doi.org/10.29302/oeconomica.2012.14.2.36
28. Wissinger, Christina L and B Gail Wilson, 'Student Perceptions of Facebook's Privacy Policies and Rights'. *Social Media Studies* 2, no 1 (2015), 15–26.
29. Wissinger, Christina L, 'Privacy Literacy: From Theory to Practice'. *Communications in Information Literacy* 11, no 2 (2017), 378–389. Online: https://doi.org/10.15760/comminfolit.2017.11.2.9

Vivien Kardos is a PhD student at the University of Szeged, Faculty of Law and Political Sciences, Department of Statistics and Demography. In her research she focuses on the use of artificial intelligence in law by a practical view, which includes the opportunities, challenges and risks as well. Moreover, she is particularly interested in analysing AI from a data protection perspective. Further to this she has already published several articles on digital competences of law students, which is another area she is interested in.