# INSIGHT INTO THE PERCEPTION OF PERSONAL DATA AMONG LAW STUDENTS

Vivien Kardos[1]

**DOI: 10.24989/ocg.v.338.10**

***Abstract***
*In the period of the fourth industrial revolution, it can be established that the issue of data protection has become more important than ever before. There is no doubt that data, especially personal data represents a significant commercial value. Additionally, it has many impacts for the legal profession. In accordance with the increasing role of data protection, the question arises whether law students have appropriate knowledge of privacy literacy.*

*Based on the results of empirical research, this study has demanded a response to the question of what their attitudes are towards the importance of their personal data, how it works in practice, when, for example, using various kinds of social network sites, and which data protection guarantees are known by them. 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, which can be ascertained from the findings of the preliminary quantitative research.*

*Anticipating, it should be emphasised, that law students are not 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 concerning health. Consequently, the privacy literacy of law students needs to be improved.*

## 1. Introduction

According to the latest publication of *Internet World Stats*, there are approximately 4.54 billion Internet users worldwide.[2] (Internet World Stats, 2019) Nowadays it is not a recent establishment that the use of social media platforms is ordinary among the life of 'digital natives'. (Prensky, 2001) According to the Article 4 (1) of the 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; hereinafter referred to as 'GDPR') personal data means any information relating to an identified or identifiable natural person ('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, it has a broad interpretation, that is the reason why it is important to identify personal data in any situation.

[1] Vivien Kardos is with Department of Statistics and Demography, University of Szeged, Hungary, kardos.vivien.kata@gmail.com
[2] World total Internet users: 4,536,248,808.

In this context, the question arises as to, for instance how the perception of personal data develops among a special subject group, namely law students, who also increase their knowledge of data protection. The first question is what their viewpoint is about the importance of their personal data and regarding this question, how it works 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 are some difficulties caused because of a lack of knowledge of the broad interpretation of personal data. Moreover, the question is why the perspective of law students has been chosen to be mapped and what their attitude is to data protection and privacy in the world of social media sites.

One reason for this is that they embody future lawyers even though they are still sitting on the university benches. In this context, it is difficult to imagine that some aspects of data protection will not be encountered 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 the 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 (hereinafter referred to as 'preliminary research' or 'questionnaire') performed by the author. Some of the significant issues in connection with the privacy literacy of the law students will be shown.

## 2. What is privacy literacy?

Literacy can be defined with the fusion of two terms, which are knowledge and skills. (Sideri et al., 2019) The concept of digital literacy may seem to have the same sense as privacy literacy, notwithstanding it should be emphasized that there are significant differences between the two terminologies. The term of privacy literacy is focused on the understanding of the responsibilities and risks associated with sharing information online, on the contrary digital literacy focuses on the task-based use of information in a digital environment. (Wissinger, 2017)

Privacy literacy is *'the understanding that consumers have of the information landscape with which they interact and their responsibilities within that landscape'*. (Langenderfer & Miyazaki, 2009) Another point of view *Trepte et al.* stated that online privacy literacy is a combination of declarative and procedural knowledge. (Trepte et al., 2015) From the point of view of developing the data protection of the students, privacy literacy has many useful aspects, for instance it is a good basis for strengthening online privacy. (Bartsch & Dienlin, 2016) Research has highlighted the users' lack of knowledge and skills to protect their privacy. (Park, 2011)

*'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.'* (Sider et al., 2019) 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'. (Givens, 2015) The question could be raised as to precisely which skills are included terms of privacy literacy. At present there is no sanctioned list of privacy literacy skills concerning this issue. (Wissinger, 2017)

## 3. Background – the preliminary research

### 3.1. Method

Before presenting the research on which this study is based, it is important to emphasise the factors that have contributed to and have warranted the conduct of the research detailed as follows. The questionnaire, which was carried out on a voluntary basis, was conducted on an online interface, with a total participation of 205 law students from all eight Faculties of Law in Hungary. The majority of them were full-time students, involving all years from the freshman year to the final year. Moreover, some correspondence students also took part in order to broaden the investigational spectrum. The data collection took place at the beginning of 2020. This questionnaire covered several fields of data protection and privacy literacy.

With regard to the structure of the questionnaire, which included themes of general data protection and the usage of social network sites (hereinafter referred to as SNSs), it is primarily related to the sharing and accessibility of personal data. Without mentioning all of the issues, it can be stated that it also comprises topics of daily usage of SNSs, password protection of digital devices and personal data breach. The key consideration in the creation of the questions was to be able to use them for measuring knowledge, attitudes and habits. To achieve real results, there were some questions related to practical life, such as what types of personal data are shared on SNSs. Among the questions, some of them pertained to single and multiple responses in the form of direct and indirect questions. Furthermore, scales of one to ten were also used.

### 3.2. Main findings

Apart from a detailed analysis of the results, the main findings of the questionnaire can be determined as follows: Although the recognition of the importance of data protection appears among law students, their "activity" on SNSs is not fully accordance with their statements. Approximately 95% of respondents use some form of SNSs on a daily basis. Not surprisingly, Facebook is the most common, however, nearly three quarters of them do not read the privacy policy at all. This is also decisive in terms of attitude.

One of the most remarkable results of the preliminary research is that it can be established that identifying personal data through practical examples causes difficulties for law students. In this context, significant gaps can be established in relation to data concerning health, as well as in the case of the cookie identifier (hereinafter referred to as 'cookie ID'), so it became justified to ask additional questions to law students in order to shed light on the underlying causes.

Knowledge gaps were also revealed in connection with the cookie ID, which will be presented in detail afterwards, given that the highest error rate was in the case of this kind of personal data, and contradictory results were obtained. Anticipating, it can be stated that most of the law students basically do not have knowledge of what exactly 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 and achieve a broader scope of research, sixteen in-depth interviews were conducted with two law students from each of the Faculties of Law[3] in Hungary. It should be emphasised that the interviews were conducted with the voluntary consent and participation of the interviewees, and the information was used anonymously. The interviews were conducted with the aid of a telecommunication tool, the interviews lasted an average of 18 minutes.

The age of the interviewees, who attend different years at the universities, ranges from 21 to 29 years, the average age is 22.81 years. The gender distribution more or less can be considered as balanced, considering that nine men and seven women were interviewed. The questions focused on assessing privacy practices, attitudes, and the knowledge of law students in the context of the mentioned gaps.

### 4.2. Results

Before analysing the in-depth interviews, it should be noted that the vast majority of the respondents have already heard about certain aspects of data protection in university courses. In this regard, the degree to which the depth is divided is that the students could only tangentially gain knowledge or gain experiences in the courses of semesters over a number of years. The responses 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 had a course specifically on data protection.

Additionally, all of them stated that they had already encountered data protection beyond the university walls in several situations. Examples include writing research papers in the field of data protection, internship in law firm regarding data protection matters, participation in a briefing at the National Authority for Data Protection and Freedom of Information (hereinafter referred to as 'The NAIH') or even approving the data processing policies, other briefings and regulations on the social media platforms. All interviewees use Facebook and 13 of them also use Instagram daily. Furthermore, LinkedIn, Snapchat and Reddit were also mentioned on occasions.

#### 4.2.1. 'Is it personal data?'

Based on the results of the preliminary research, it became evident that through practical examples, the identification of personal data, particularly cookie ID, and data concerning health[4] have posed difficulties, thus eleven pieces of information were presented during the interview. These were the following information and personal data: Cookie ID; a medical prescription that must be purchased at a pharmacy; the advertising ID of 'your' mobile phone; the IP address of 'your' laptop; cell phone location data; X-ray of 'your' broken tibia; sonogram of your internal organs; the company registration number of the commercial service company in 'your' place of residence; ID number on the residence card; 'your' own address; diagnosis on the outpatient information sheet. Most of these were mentioned in the preliminary research.

---

[3] DE-ÁJK, ELTE-ÁJK, KRE-ÁJK, ME-ÁJK, PPKE-JÁK, PTE-ÁJK, SZE DF-ÁJK, SZTE-ÁJK

[4] 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.

In accordance with results of the questionnaire, it can be seen that the address, and the diagnosis on the information sheet is obvious for approximately 93% of the respondents. It should also be noted that there were no examples when all of the law students knew the correct answer. That is also thought- provoking, because these were the easiest ones. However, the ‘not typical’ kind of personal data, for instance cookie ID or the IP address of the laptop, is more difficult not to mention the advertising ID of the mobile phone or the cell phone location data. That is the reason why the majority of the law students selected and stated the wrong response.

It became apparent that the identification of personal data is a real challenge for law students, when ‘not typical’ personal data should be identified. Interviewees gave different responses to similar data concerning health, thereby confirming the uncertainty of their knowledge in connection with personal data. All of the interviewees knew that diagnosis on the 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 are also personal data. These questions pointed out that they did not have knowledge even though the aforementioned four examples are personal data, particularly data concerning health. A significant difference could be established – over 13% – in 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 one was the cookie ID, that the majority of students’ point of view is 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 personal data, which is considered as the most personal data (hereinafter referred to as ‘most personal data’). It was a separate question concerning the attitude of the law students to the 'most personal data' that they still share or would share on social media platforms and the ones that are so personal that they do not share at all. The responses were quite varied, showing significant differences.

The telephone number and the email address are closely related to the interviewees' privacy, as the vast majority of them are not shared on social media platforms, although, one of the interviewees shares both with their friends. Based on the research most of the interviewees share their date of birth and their university on these platforms. One of the interviewees stated that she would not share her educational background. The responses are indicated that most of the interviewees share their place of residence, but not the exact address. In this context, it is important to mention that three students do not share the location where they exactly are, for instance a holiday abroad, because they are afraid of a burglary. It should be emphasised that this process shows knowledge and appropriate action too, 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 also share their identity card number on SNSs. Contrary to this viewpoint, the other interviewees stated that they had not shared any personal documents and cards at all.

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

4.2.3. Issue of the ‘cookies’

The question could be raised as to why this issue is so important. The questionnaire showed that law students have an incomplete knowledge in this field of personal data, and conceptual disorders can also be identified. This theme is considerable from the perspective of knowledge and attitude too. Bearing in mind that cookie ID has an extremely close relation to data protection and law students could encounter many examples of it every day, that is the reason why it has been given a prominent role in the preliminary research.

One of the main findings is that law students often encounter pop-up ‘cookie-windows’ in everyday life and most of them could determine the meaning of it by choosing the right response from the alternatives. Notwithstanding, there are significant shortcomings in the evaluation of their operation and legal nature. Given that 87 percent 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 be originated from. The first question is related to the habits of the interviewees whether they would accept cookie policies and allow cookies. With the exception of two respondents, all interviewees accept them, but significant differences can be established between the underlying reasons.

One of the two negative responses have inherent privacy, data protection reasons and the other one has a convenience role, as the interviewee stated that they did not consider it important, it was just slowing down the sites. The other answers were basically about streamlining the browsing experience. Furthermore, articles cannot be read, or the person is not able to move on to the websites without acceptance. Four of them indicated that they were otherwise aware of the consequences. One interviewee pointed out that he used to delete all of the cookies monthly, while others minimized 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 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 correct response rate of 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 percent of the law students indicated cookies as ‘risky’ from the point of view of privacy. Therefore, interviewees were faced with the question of whether they had a privacy concern in connection with cookies and given their way of reasoning. The open-ended question provided an opportunity to visualise, in the light of the reasoning, how broad the spectrum of the interviewees’ opinion is. Seven interviewees responded that they had already thought about privacy concerns in the context of cookies, 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 with the utilisation

of their personal data. Two respondents inferred from the question that they probably have, however they also noted that they had never been interested in this theme enough to look for 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 considered that is was a huge mistake on his part and he stated that he should have read up on this subject.

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

Confirming the results of preliminary research, it can be stated that there is a significant lack of knowledge of many law students regarding cookies. They give their consent without even knowing what it is exactly, and this could make efficient data protection difficult. Moreover, this attitude is likely to manifest itself in other cases as well. This question is not new because according to *Conger* the students voluntarily provide this consent without any consideration to its collection, and ignoring that information is currently not under their control, but under the control of the organisations that possess it. (Conger et al., 2013) Furthermore, many of them are not interested in what happens with this information.

4.2.4. Personal data breach

During the interviews law students were questioned whether they had already had a personal data breach and in general what their knowledge is about its meaning. According to the Article 4 (12) of the GDPR the 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 restricted, it was shown by the examples. Only one student stated that it could happen accidentally, without bad faith. In all other cases, the unlawfulness appeared in connection with the personal data breach. 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 the personal data by third party, misuse of personal data, unauthorised data transfer, and unauthorised use of a telephone number. One interviewee pointed out that he has not heard of this legal term at all, which also draws attention to the need to increase awareness, as on the one hand, the personal data breach has to be recognised before taking any further actions.

The main finding of 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 have a lack of knowledge in this field. The importance of this issue is that if the 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 it can happen accidentally.

4.2.5. Data protection guarantees

As referring to the preliminary research the majority of the law students cannot list 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 knowledge needs to be extended and recounted as soon as possible. A separate question is designed to measure the knowledge and awareness of the law students, namely what kind of data protection guarantees they have known. The preliminary assumption which they referred to was for example the principle of purpose limitation or the right to be forgotten. None of them were expressed, only two respondents stated the necessity of consent, and the acceptance of privacy policy statements.

Seven interviewees stated that they could not, had not remembered, or had not learnt in depth to remember it. Six students mentioned examples of the European and national legislation in connection with this issue. It should be noted that a 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. It could seem to be just one answer, but the respondent is probably not alone with this lack of knowledge, which is also important to establish. In addition, the NAIH was listed in two cases, although it should be noted that in both of them its full name was determined 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. (Wissinger & Wilson, 2015) This establishment can be underlined in general.

Notwithstanding, eleven interviewees stated that nowadays, considerably fewer photos, posts and comments are shared on social media platforms by them 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 had also changed, according to them they want to share fewer 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

Nowadays, it can clearly be established that personal data is becoming more and more valuable. In order for data protection guarantees to prevail, it is essential for individuals to pay attention to data protection in their daily habits as well. All interviewees acknowledged the importance of data protection, nevertheless considerable differences were shown in the degree to which the interviewees have knowledge of privacy literacy. In support of the questionnaire, it can be stated that the identification of personal data through practical examples is difficult for law students.

The results of the research have shown that the field of privacy literacy needs to be improved in order to achieve an even higher level of data protection with appropriate efficiency for law students. Improvement of the existing knowledge and developing the shortages of privacy literacy is essential. Overall, based on the results, it can be stated that law students have only superficial knowledge in many areas of data protection, they have difficulties with it and the existing knowledge has not been properly adapted in practice.

The 16 in-depth interviews, together with the preliminary research of the total participation of 205 law students, are suitable for establishing a pattern and raising further research questions, such as how

well students are aware of the data protection risks and possible consequences. In addition, less self-evident deficiencies in knowledge may have surfaced so far. Given that, presumably due to the profession, law students pay more attention to data protection, it is likely that the average university students do not reflect on this. In order to develop privacy literacy, it is necessary to present practice-oriented knowledge in education as well, so that law students can apply their knowledge properly in practice.

## 6. Acknowledgement

This research was supported by the project nr. EFOP-3.6.2-16-2017-00007, titled Aspects on the development of intelligent, sustainable and inclusive society: social, technological, innovation networks in employment and digital economy. The project has been supported by the European Union, co-financed by the European Social Fund and the budget of Hungary.

## 7. References

[1] BARTSCH, M. and DIENLIN, T., (2016). Control your Facebook: an analysis of online privacy literacy. *Computers in Human Behavior,* 56, 147–154.

[2] CONGER, S., PRATT, J. H. and LOCH, K. D., (2013). Personal information privacy and emerging technologies. *Information Systems Journal,* 23(5), 401–417.

[3] CORREIA, J. and COMPEAU, D., (2017). Information privacy awareness (ipa): A review of the use, definition and measurement of IPA. *In Proceedings of the 50th Hawaii International Conference on System Sciences,* Waikoloa, HI.

[4] GIVENS, C. L., (2015). Information privacy fundamentals for librarians and information professionals. New York, NY: Rowman and Littlefield.

[5] INTERNET WORLD STATS: World Internet Usage and Population Statistics. 2019 Mid-Year Estimates, 30 June 2019 (Retrieved from https://www.internetworldstats.com/stats.htm – 06. 01. 2020.)

[6] LANGENDERFER, J. and MIYAZAKI, A. D., (2009). Privacy in the information economy. *The Journal of Consumer Affairs,* 43(3), 380–388.

[7] PARK, Y. J. (2011). Digital literacy and privacy behavior online. *Communication Research*, 40(2), 215–236.

[8] PRENSKY, M., (2001). Digital Natives, Digital Immigrants. *On the Horizon*, MCB University Press, 9(5), (Retrieved from https://www.marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf – 28. 12. 2019.)

[9] 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)

[10] SIDERI, M., KITSIOU, A., TZORTZAKI, E., KALLONIATIS, C. and GRITZALIS, S., (2019). Enhancing university students' privacy literacy through an educational intervention: a Greek case-study. *Int. J. Electronic Governance*, 11(3/4), 333–360.

[11] TREPTE, S., TEUTSCH, D., MASUR, P. K., EICHER, C., FISCHER, M., HENNHÖFER, A. and LIND, F., (2015). Do people know about privacy and data protection strategies? Towards the 'online privacy literacy scale' (OPLIS)'. in: Gutwirth, S., Leenes, R. and de Hert, P. (Eds.): *Reforming European Data Protection Law*, Springer, Heidelberg, Germany, 333–365.

[12] WISSINGER, C. L., (2017). Privacy Literacy: From Theory to Practice. *Communications in: Information Literacy.* 11(2), 378-389.

[13] WISSINGER, C. L. and WILSON, B. G., (2015). Student perceptions of Facebook's privacy policies & rights. *Social Media Studies* 2(1), 15–26.