Data Privacy Aspects of E-learning

Tanya Pehlivanova[1], Kamen Kanchev[2]

(1) Trakia University–Stara Zagora, Faculty Technics and Technologies - Yambol, 38 "Graf Ignatiev" str, Yambol - 8602, Bulgaria
E-mail: tanya.pehlivanova[at]trakia-uni.bg
(2) New Bulgarian University, 21 "Montevideo" str, Sofia – 1618, Bulgaria
E-mail: kamenkk[at]abv.bg

Abstract

In today's world distance learning is increasingly used. Web-based tools are used to implement it. In order to function properly, they must store information about their users. This paper goes through the issue of data confidentiality when using e-learning. A study among students from Trakia University - Stara Zagora, Bulgaria is presented. It aims to check whether students are aware of how their personal data is used and what is their sense of security for personal data while using e-learning platforms. The students' attitude to the personal information that they are predisposed to share with the other participants in the e-learning courses is studied. It was concluded that a large number of students are not aware of the problems that can arise from sharing personal data and how they and the lecturers can protect their data. In addition, confidentiality recommendations have been proposed that should be taken into account when using e-learning.

Keywords: Data privacy, e-learning, Distance learning, Personal data

1. Introduction

A trend in modern education is the growing role of distance learning. Distance learning provides a unique opportunity to acquire education, without the physical limitations associated with the location of the educational institution, the lecturers and the learners. It can be used independently, but it can also be a complementary training to traditional forms of training.

Modern distance learning uses web-based learning management systems (LMS). Often it is done asynchronously by providing digital materials for reading, video and audio recordings for watching or listening in the student's free time, discussion forums and chats. With the development of technology, synchronous technologies are increasingly being used, including live video or audio connections.

LMS are the tools with which distance learning is carried out. They have indisputable advantages, such as: saving time aond money for travel, 24-hour access to training materials, one-time creation of courses that can be used and improved at any time, rich opportunities for creating tests and assessment, etc.

Distance learning became especially relevant during the pandemic with COVID-19, due to which all pupils and students were forced to switch to online training.

In order to function properly, LMS needs to store information about their users. Since they are information systems that manage personal information, they must comply with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council GDPR.

GDPR is an EU regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (Regulation (EU), 2016). It was adopted in April 2016 and is applicable from May 2018. This Regulation protects the fundamental rights and freedoms of individuals and in particular their right to the protection of personal data.

The personal information that is entered in the LMS includes name, surname, email address, profile image along with others. In addition, LMS store personal information about students' progress, such as students' grades for each course and activities they have taken online.

LMS registers every action of students, logging in and out of the system, length of their session, read materials, posts in forums and chats.

Much of this information is available not only to system administrators and course instructors, but also to students enrolled in the course. In many online courses they can see a list of all enrolled in the course students, information from their profile - photo, email, etc., links to their profiles on social networks, the activity of students in the course, records from forums and chats and last but not least course grades.

The design of the LMS in terms of data privacy protection can lead to cyber harassment, among other inappropriate behaviors (Kambourakis, 2013; Mayes et al, 2015; Amo et al, 2020) .

In order to use an e-learning platform, the student is obliged to accept its conditions, in which the policy for personal data processing should be described. He has no right to refuse, as this would mean that he would lose access to the desired training.

To protect students' identity from other students, various technological measures have been proposed. For example, (Anwar and Greer, 2015; Amo et al, 2020) propose solutions by introducing anonymity to participants.

Another problem that arises when using LMS is insufficient confidentiality on the part of the leading lecturers in the course. They often use the e-learning system to communicate with students, to provide information, messages to students in which they unintentionally disclose sensitive students information. For example: uploading lists with grades from exams and course assignments that have not been conducted in e-learning, lists of students who have not completed assignments, attendance sheets, etc. Sometimes in these lists are used identification numbers of the students instead of their names. However, this is not enough. The identification (faculty) numbers can be easily learned by all students, especially in universities where training is carried out in groups with a small number of students. Most often this happens from lists in the LMS containing the names together with the numbers of the students.

Often, to carry out distance learning platforms are used, with the help of which a video connection with students is made (Zoom, Google Meet). Most of these platforms require at least the name and email addresses of students and lecturers. This is necessary for the platform to manage identification, accounts and logins. Platforms may also collect data through cookies or other online identifiers. This information may be obtained by third parties and used for innocent purposes, such as targeted marketing, but may be resold or used by malicious persons to obtain personal information about users or even identity theft.

Most articles related to data confidentiality when using e-learning are aimed at reviewing existing technological solutions to ensure data confidentiality and offering new solutions (Jerman-Blažič, 2005). There are also publications that examine the satisfaction of students and lecturers with the privacy of data in the LMS.

In (Ivanović et al, 2013) it is said that „Regarding possible privacy issues, the majority of students are satisfied with the privacy level offered by Moodle, though they gave specific remarks and expressed their general opinion that access to their private data should be limited. Teachers, on the other hand, seem to have no privacy concerns whatsoever. When asked which parts of the information from the user accounts should be hidden, expected answers were received such as e-mail addresses, telephone numbers, identification numbers, etc. Some students also mention hiding first/last access times and activity diaries of course participants.

The answers to the questions „What kind of privacy data is enough for educators to manage a successful learning process?“ and „What kind of data the students are predisposed to share in order to successfully accomplish their learning activities?“ were found in (Ivanova, 2015). A model for protection of users' privacy combining components of different measures and actions - technical, institutional, legal, educational, social and economic model is proposed there.

The technological measures related to the collection of personal data necessary for the qualitatively conducting the training, as well as for the security of the information used are discussed in (Jerman-Blažič, 2005; Romansky, 2019). This paper examines only the attitude of students to the personal information they are predisposed to share with other participants in e-learning courses.

The aim of the paper is to examine whether students are familiar with how their personal data is used and what is their sense of security about personal data while using e-learning platforms. In addition, privacy recommendations have been proposed, which should be taken into account when using e-learning.

2. Methods

To achieve the goals of the paper, a survey was conducted with 94 first and second year students from the Faculty of Technics and Technologies-Yambol, studying in technical programs. The survey was published in two electronic courses - "Electrical Engineering and Electronics" and "Theoretical Electrical Engineering" in the learning management system Moodle. The surveyed students have experience with the use of courses in the e-learning system and can express a competent opinion.

The survey includes fourteen questions. They are related to the risks of leakage of personal information when using the e-learning system. It examines what personal information students are prone to share with administrators and other course participants. Are they concerned that other students might have access to their personal information such as email, enrolled courses and activities, grades, opinions posted in chats, forums, video recordings of lectures or exams , in which they participated, etc.

3. Results

The majority of surveyed students (56.38%) believe that they are aware of the risks of leakage of personal information when using the e-learning system or other platforms for distance learning. Approximately the same number of students claim that they know what personal data the other participants in the courses have access to.

At the same time, 41.49% admit that they do not know this (Figure 1).

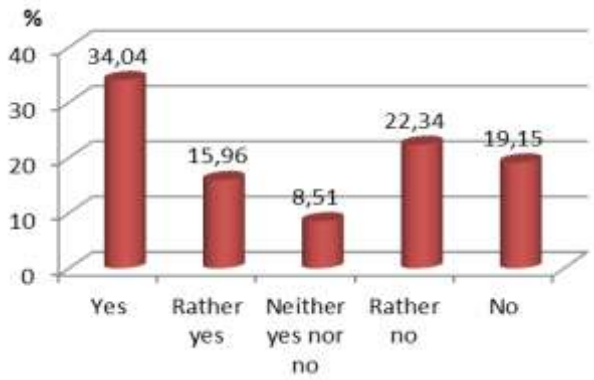

Figure 1. Are the respondents aware of what personal data the other participants in the courses have access to?

Only 23.4% of the respondents do not feel secure about their personal data while using the e-learning system or other platforms for conducting distance learning (Figure 2).

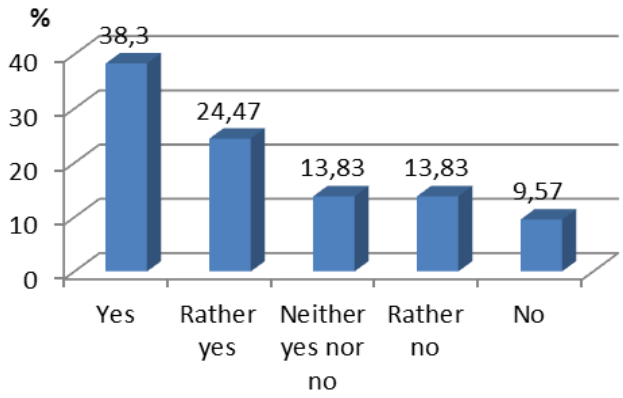

Figure 2. Sense of security for personal data at conducting e-learning

The predisposition to share different types of personal data has been studied - grades, emails, enrolled courses and activities in them, posts in forums and videos in which students participate.

About two-thirds of respondents are not worried about the fact that other students may have access to their grades, their participation in forums, and videos with their participation. Slightly smaller is the percentage of those who do not worry about sharing information about enrolled courses and actions in them and their emails (Figure 3).

A similar result regarding the sharing of assessments was obtained in (Ivanović et al, 2013). Some Serbian students even want to see their colleagues' grades as a way to improve the transparency of grades.

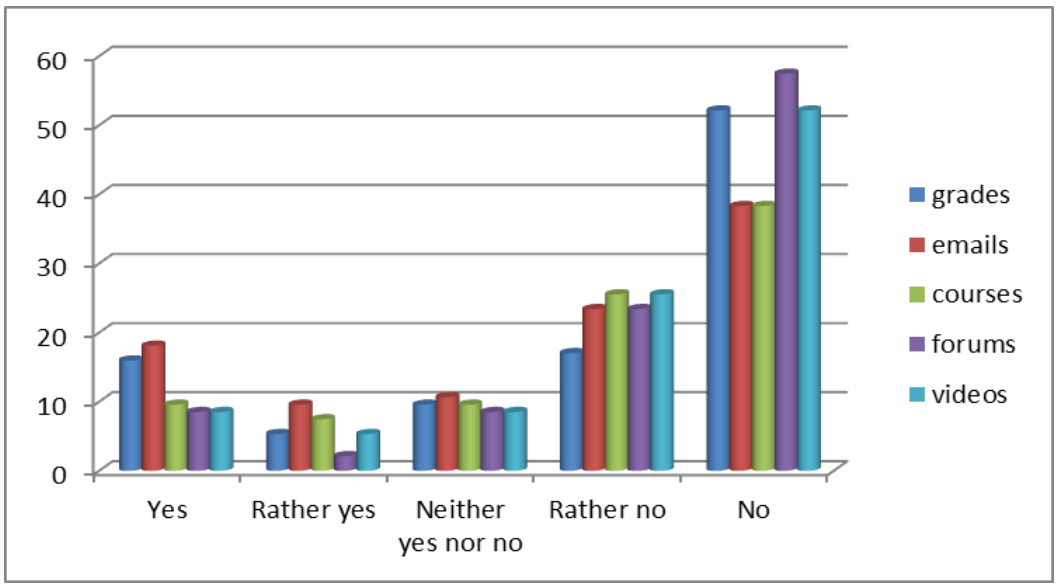

Figure 3. Predisposition to share different types of personal data

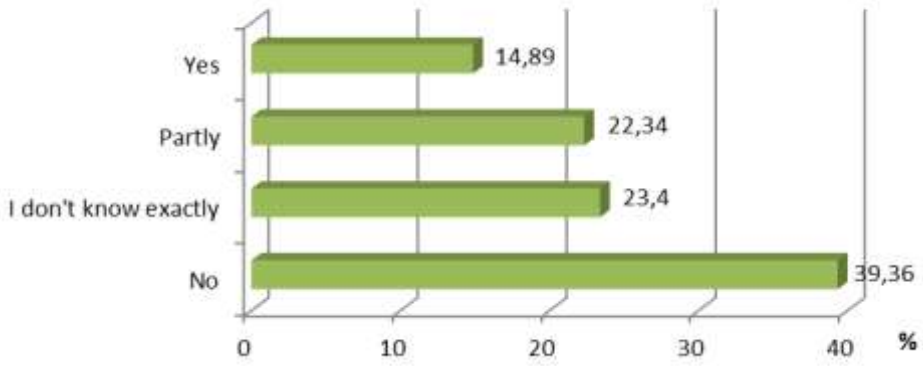

Figure 4. Are students familiar with the European regulation on personal data protection?

The probable reason for the high sense of security and predisposition to share personal information is that a large number of students are not sufficiently aware of which data is personal and which data they have the right not to share. They are not familiar with EU legislation on the protection of individuals with regard to the processing of personal data. To the question "Do you know what GDPR is?" Only 14.89% answered positively. 22.34% are partially familiar, and 39.36% - answered negatively (Figure 4).

This explains the high percentage of respondents who do not think that they themselves should determine what data they can share with other participants in e-learning courses. 85% are convinced that the University does what is necessary to protect their personal data.

After analyzing the most common ways to access personal data when using e-learning, the following non-technological measures to preserve the privacy of student data are formulated:

- The courses should be re-created every year so that students do not have access to information about the old participants and documents published for / by them;
- The access of already graduated / dropped out students to LMS should be suspended;
- Students should use institutional email addresses, instead of personal ones;
- When sending mass emails and messages to a larger group of students, the blind carbon copy (Bcc) option should be used for listing the recipients so that information about grades, course participation, etc. cannot be retrieved from the address list. If possible, pre-created email groups should be used;
- Files containing general information about the students in the course should not be published;
- Video recordings should be made only with the consent of the students and they should be allowed to work without using cameras, if this is not necessary for the purposes of the course or as a security measure during the exam / current control;
- The lecturers to explain to students the risks of excessive sharing of personal data;
- To give students the opportunity to request deletion (hiding) of information published by or about them in already completed courses;
- When publishing papers by previous course participants, as an example of a task, data such as identity numbers, emails and grades / reviews must be hidden, unless if the students have not agreed their data to be distributed in this way;

- When conducting a videoconference, use the options of the system used to approve the participants in the videoconference in order to avoid the participation of unauthorized persons in it, which in turn may lead to leakage of personal information;
- The latest versions installed from authorized sources on all software systems used, both LMS and videoconferencing to protect against data leakage through vulnerabilities in the software must be used.
- When conducting a videoconference, the microphones and the camers of the participants should not be enabled by default. If this is necessary, the students should be clearly informed in the invite for the meeting.

4. Conclusion

This paper presents the results of a survey among students from the Trakia University - Stara Zagora, Faculty Technics and Technologies-Yambol on issues related to the privacy of personal data in the application of distance learning.

The results show that almost all students feel secure about their personal data in e-learning. They are convinced that the University is doing what is necessary to protect their personal data. Most of them, however, do not know what personal data the other participants in the e-learning courses have access to and are not aware of the problems that may arise from sharing personal data in them.

The attitude of students to the personal information that they are predisposed to share with other participants in e-learning courses was studied. About two-thirds of respondents are not worried about the fact that other students may have access to their grades, their participation in forums, and videos with their participation. Slightly lower is the percentage of those who don't worry to share information about enrolled courses and actions in them and their emails.

The paper also makes privacy recommendations that should be taken into account when using distance learning.

References

Amo, D., Alier, M., García-Peñalvo, F., Fonseca, D. and Casañ, M. (2020): Protected Users: A Moodle Plugin To Improve Confidentiality and Privacy Support through User Aliases. *Sustainability* 12, 6, Article 2548.

Anwar, M. and Greer, J. (2015): Facilitating Trust in Privacy-Preserving E-Learning Environments. *IEEE Transactions on Learning Technologies* 5, 1, 62-73.

Ivanova, M., Grosseck, G. and Holotescu, C. (2015): Researching data privacy models in eLearning. In *Proceedings of The International Conference on Information Technology Based Higher Education and Training (ITHET)*, Lisbon, 1-6.

Ivanović, M., Putnik, Z., Komlenov, Ž., Welzer, T., Hölbl, M. and Schweighofer, T. (2013): Usability and Privacy Aspects of Moodle - Students' and Teachers' Perspective. *Informatica* 37, 221–230.

Jerman-Blažič, B. and Klobučar, T. (2005): Privacy provision in e-learning standardized systems: status and improvements. *Computer Standards & Interfaces* 27, 6, 561-578.

Kambourakis, G. (2013): Security and Privacy in m-Learning and Beyond: Challenges and State-of-the-art. *International Journal of u- and e- Service, Science and Technology* 6, 3, 67–84.

Mayes, R., Natividad, G. and Spector, J. (2015): Challenges for Educational Technologists in the 21st Century. *Education Sciences* 5, 221–237.

Regulation (EU) 2016/679 of the European Parliament and of the Council GDPR (2016): https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679, accesed 2020

Romansky, R. and Noninska, I. (2019): Technological organization of the access management to information resources in a combined e-learning environment. *International Journal on Information Technologies & Security* 11, 4, 51-62.