Problems of Privacy and Data Protection in Online Learning Based on the Network Space

Radi Romansky

Abstract: *The article presents opportunities proposed by global network space for realization online learning, sharing information resource and communications between users. These network activities are connected to the creation of personal profiles and uploading personal information that could be accessed by other users, not always in a correct way. In this reason some important problems for user's privacy based on the European legislation for personal data protection are discussed.*

Key words: *information society; privacy; personal data protection; e-learning.*

INTRODUCTION

Lifelong learning (LLL) is an important key characteristic of contemporary Information Society (IS) and is realized by using Information and Communication Technologies (ICT). One of the important elements of LLL is the online learning described in general as a method for exchange of information resources and knowledge through the global network space. It is possible to ask the question "What are the components of network space?" Traditional component of course is the web-environment that proposes large collection of contents, specific and traditional learning resources, tools for virtual reality, etc. that could help learners obtain some knowledge based on interactive communications. This collection of means and tools could be extended by opportunities of social media and Web 2.0 tools that permit collaboration and sharing of information and knowledge between large set of users. In other hand social media gives different point of view of LLL because it allows users to create personal learning content and organize the collaboration on the base of specific interests [1]. Another aspect of online learning is Massive Open Online Courses (MOOCs) that many educational institutions apply. The tendency is that MOOCs will change the higher education in the next years [2]. Finally it is needed to include in this group of online learning means not only the cloud computing but also the mobile cloud computing.

Yong Chen and Wu He (USA) give in their survey [3] some statistical data for using online learning, for example "65% of higher education institutions now say that online learning is a critical part of their long-term strategy". The different means and network environments for information sharing and collaborations increase the possibilities for online learning, but we must find the answer of the question – if the personal data of users are protected and if the principles of privacy are respected. Fact is that social media and cloud computing give different opportunities for collaboration, information sharing, online communications, access to information and knowledge, etc. In other hand, some important problems for personal data protection of user's profiles and posted information could be determined [4, 5, 6], and these problems are object of serious discussion in the world [7,8].

Some aspects of Personal Data Protection (PDP) and principles of privacy in the network space are discussed in this article. The main challenges of distributed environments, cloud services, social media and global communications for PDP and user's privacy are presented in the focus of European legislation and regulation documents. In this reason related work is discussed in the second section. The next sections treats the principles of privacy and data protection, features of distributed environments, social media and cloud services in focus of online learning and main problems for PDP of the network space and global communications.

RELATED WORK

It is known that e-learning offers an opportunity for remote access and using teaching materials and participation in learning process from different places in network space. This increases the importance of problems of privacy, reliability and security of e-learning systems and procedures. Learners should not lose the time for waiting for services after system failures and should have not problems with extended process of registration and security incidents. Many online learning systems have conceptual problems with principles of privacy that must be decided. The increasing access to the components of network space (web-sites, distributed resources, content, libraries, forums, social media, cloud services, etc.) requires adequate protection based on the rules of European and national data protection legislation. In this reason ten privacy principles used in Canada an e-learning standard related to privacy and security are summarized in [9]. European regulation of PDP accepts using the so called "PETs" (Privacy Enhancing Technologies) for individual protection of privacy and article [9] examines and critiques "a number of PET that can potentially satisfy privacy and security requirements for e-learning systems".

In the context of increasing global interconnections the privacy and security of e-learning could be ensured by using different encryption tools, but the main requirements should be defined as a part of data protection policy. A review of e-learning privacy and security requirements and an investigation of more popular e-learning standards are made in [10]. This article presents a typical architectural model for e-learning and used technologies as audio-video systems, websites (YouTube), messaging programs (Skype, Adobe Connect), webcams, blogging, screen casting, computers, tablets and mobile devices, virtual learning environments. The sentence "Privacy is very crucial in e-learning because user's information is needed to be secured" is the reason to discuss in [10] main principles of user and network privacy (identification, consent, trust management) and security mechanisms (authentication, confidentiality, user ongoing session authentication).

A study on user's perception in using e-learning technologies and the awareness-raising of security and privacy issues is made in [11]. The authors note that the learning environments have different security and privacy levels that depend on types of learning activities being conducted by the participants, but each learning system must protect sensitive personal data of the learners. The article includes results from a survey that has been conducted to study the urgency of different protection measures. The investigated parameters of privacy are PDP, anonymous use, address and location policy, single sing-on, seamless access, authentication, Digital Rights Management, legislation, awareness raising. A conclusion is that "students requested to be able to control the visibility of their sensitive data such as history of their learning activities and their profiles".

The e-learning depends on the components of the network space that is a venue for a set of illegal activities. In this reason the protection of learners and instructors from unauthorized security threats is discussed in [12]. The concept of the article is that the e-learning security is the process of preventing and detecting unauthorized use of computer system and refers to freedom from harms such as: ✓ Corrupted or lost communications, messages, grades, data, or work; ✓ A compromised learner or instructor identity; ✓ Stolen personal or private information; ✓ Stolen or compromised student ideas and innovations; ✓ Corrupted social technical systems. In this context, the article discuses the main e-learning security threats (viruses, spyware, hackers, phishing, viral web sites, adware and advertising Trojans, online social network sites) and presents some common methods for securing e-learning systems.

The most used components of the network space to share information (including teaching materials) and to save instructional tools in data centers are social media and cloud-based learning environments. Most people (individuals and employees) use

Internet to extend their knowledge, social contacts and relationships. Social networks, forums and blogs permits to contact with different users (MySpace, Facebook, Twitter, XING, LinkedIn, YouTube, Pinterest, Foursquare, Newshub, e-Britannica, etc.) [1, 5, 6]. In other hand, the cloud permits to increase the processing and storage power by using virtual machines and storages accessed via Internet. The potential problem is that the cloud collects more and more personal information and article [13] discuses the privacy issues relevant to using cloud-based instructional tools or cloud-based teaching and learning environments for faculty members. Some instructions and practical suggestions for privacy are done. An interesting statistics for students' using web-based technologies in courses are presented, for example: 36,2 % of students use Web-based word processor, spreadsheet, presentation, and form applications (Google Docs, iWork, Microsoft Office Live Workspace, Zoho, etc.); 33,1 % use Wikis (Wikipedia, course wiki, etc.), 29,4% use Social networking websites; 16,4% use blogs and micro-blogs, etc. Three strategies for institutions to consider privacy in cloud-based teaching and learning environment are proposed in [13]: (a) legal, policy, and guidelines; (b) technical; (c) social and educational.

All these publications determine the problem with e-learning privacy and data protection as very important, so modernized regulation in using online resources in cyberspace should be applied. Some principles of privacy and PDP are presented in the next section.

PRINCIPLES OF PRIVACY AND DATA PROTECTION POLICY

The Data Protection Policy must be regarded in the context of IT Security Policy as a part of Security Policy (fig. 1). The first standard for Security Policy titled "Department of Defence Trusted Computer System Evaluation Criteria (TCSEC)" is accepted at 1985 in USA. TCSEC describes the security policy as a collection of security rules, standards, procedures, instruments and practical instructions for regulation of the management, protection and dissemination of the information. This document gives rules for control of access to the information resources.

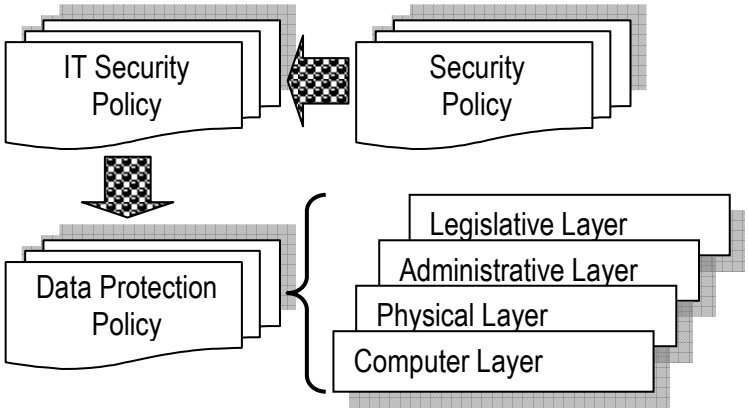

Figure 1. Data Protection Policy in the frame of Security Policy

Security Policy should be regarded as set of means and methodologies for preventing incidents, detecting attacks and restoring the system after successful attack. It includes rules, procedures and tools used on hierarchical layers (network, software, hardware, physical and administrative).

Data Protection Policy should be discussed in the frame of IT Security Policy and the European Data Protection Directive 95/46/EC outlines this relation. It is needed a harmonization of data protection with information security rules from the security core (computer layer) to the external layers (administrative and legislative). The computer layer presents embedded instruments for protection of personal data structures –

hardware, software, cryptographic, biometric. The physical layer consists of technical instruments, means and tools for unauthorized access blocking, separation of LAN segments, recognition of legitimate users, etc. The next two layers unite organizational rules, instructions and procedures for administrative control and legislative and normative documents on national and European level.

The European frame of PDP defines the main categories linked to personal dada processing:

✓ "Personal data" is information that permits to identify a person ("data subject") directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

✓ "Processing of personal data" is any operation or set of operations which is performed upon personal data by using automatic or non-automatic means.

✓ "Data controller" determines the purpose and the means of the personal data processing and is responsible for all procedure made with personal data.

✓ "Data processor" really processes personal data on the base of bilateral agreement with the controller and realizes the main goal and procedures for data processing (the controller has the main responsibility to correct personal data processing).

Data Protection Policy principles reflect on the System for PDP that should be realized by data controllers as a collection of technical and organizational measures [7, 8]. Figure 2 shows architecture of that system from the point of view of data protection in the online learning. Input point of the system should be Digital Rights Management System (DRMS) that realizes some important components of IT Security Policy:

- Authentication – it could be made by using username and password or by digital certificate, personal identification number, dialog, etc. Biometric means and tools could be used for access to the sensitive personal data.
- Authorization – this is an important component of the protection policy related to development of digital right management system.
- Accountability – the goal of this function is to personalize the access to the data structures and make a registration of users' activities, and to make continuous control for all accesses with finding solution to eventual problems.
- Integrity and content management – assuring correct, precise and actual information in the registers with personal data.
- Intelligent web-forms – a possibility for using remote access to the forms for data controller's registration, business information actualization and other on-line activities that is connected with the e-governance principles of the European Union.

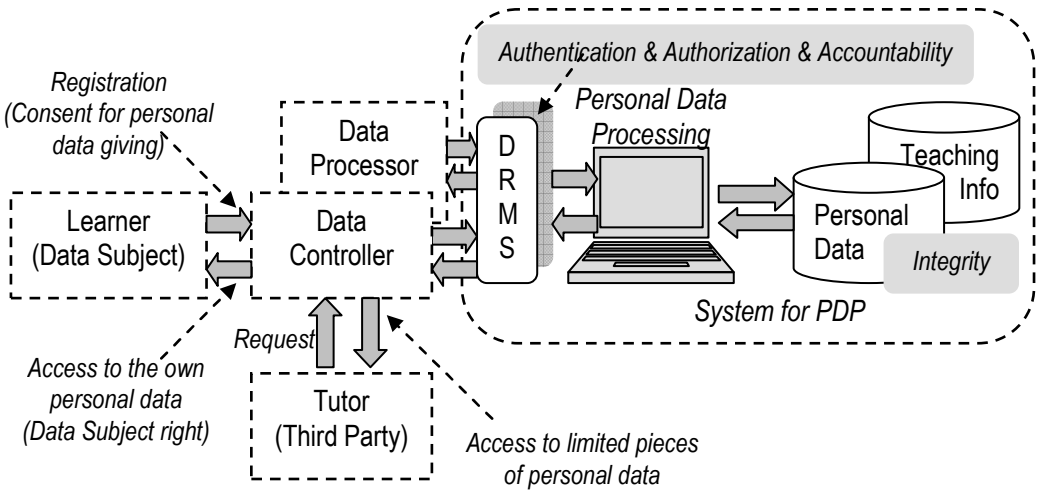

Figure 2. Architecture of System for Personal Data Protection

PRIVACY AND DATA PROTECTION PROBLEMS IN THE NETWORK SPACE

The main security concept is that the legitimate participants in online learning should be enabled to connect whenever and wherever they like. In other hand access of all illegal users must be rejected or restricted by including in special set of IP-addresses and automatic logout with destroying the session. This functionality should be provided for the e-learning system. The problem could be the fact that all components of network space permit multi-user access and several users could use one computer. Administrators (data controllers) should determine personal user's accounts and users must identify themselves before start working with the system. In addition the roles of moderators and participants must be separated in order not to provoke illegal interest to the profiles and sensitive data. In this respect data protection policy (see fig. 1) has two aspects – formal (technical oriented rules and procedures) and informal (rules concerning human behaviour). Some master data are required by the system to manage learning processes that are separated in three groups - common contact information (e-mail address, postal address, phone number), personal data (date of birth, nationality or native language), administrative data (learner ID, list of selected courses or modules, results of completed courses). Some of these data are sensitive (personal data and results from completed courses) and tutors should access only contact data for direct communication. All these requirements evoke the problems listed below.

✓ The roles of participants in online learning process ("Data Controller", "Data Processor", "Data Subject") must be defined clearly in order to determine the responsibility for PDP procedures and to keep data subjects rights. The problem in network space (web-sites, forums, social media, clouds, etc.) is that the functions of customer, vendor and provider and the relation between them could be defined for concrete case only and this permits to ignore obligations to the personal data during collection, support and transfer to third party.

✓ All data subject's right provided by European PDP regulation documents must be kept. For example, some network sites collect extended personal information (social life, gender, hobbies, relationships, etc.). Another problem is the impossibility to revise, access, block and delete their personal data (fundamental right guaranteed by the EU law). In other hand, the providers have a full access to the customer's data and the data controller must guarantee adequate prevention for unauthorized access and incorrect dissemination of personal information.

✓ The data transfer is very important obligation of the data controller because Directive 95/46/EC requests that personal data could be transferred to third party or country if it is has consent of owner and the country has adequate PDP to those of EU countries. It is possible to exist a problem of data transfer between different service providers (social media) or data centers (clouds) located anywhere in the word.

✓ The users have the right to request a deletion of their personal data for different reasons but they will not know if the data are actually deleted. The problem is that some copies of personal data could be stored in different network nodes after transferring. Data protection legislation gives strong rules for deletion of personal data in the traditional cases, but for the social media this is not clearly determined.

✓ The information in network space (including personal) could be shared and accessed from different places in the world. This poses a threat as loss data, destroying the integrity, problems with accountability, hacker's attacks, etc., and data subject does not know what policy and measures are used for counteraction to eventual attacks.

✓ Main obligation of data controller is to provide technical and organizational measure for data protection by building System for PDP (see fig. 2). These measures must restrict everybody form of illegal processing, transferring and unauthorized access.

CONCLUSIONS

The problems of users' privacy in the Internet-world and the protection of their personal information is very important theme and new regulation of the legislation should be made. In this reason the European Commission has proposed new rules to strengthen online data protection rights ("Proposed Regulation", January 2012). The European Parliament has extended this activity by adopting on 12th March 2014 some architecture and fundamental principles for data protection reform for improving user's protection and security in cyberspace. A new paradigm "the right to be forgotten" has been introduced. The new principles of regulation must extend the PDP frame determined by the previous directives for adequate and effective PDP in the network world. In other hand, the users should undertake personal measures to protect their own information in the network space (social media, Internet cafes, blogs, websites, libraries, forums, clouds, etc.)

REFERENCES

[1] Neville, K., C. Heavin (2013). Using social media to support the learning needs of future IS security professionals. Electronic Journal of e-Learning, 11(1), pp.29-38.

[2] Meyer, J.P., S. Zhu (2013). Fair and equitable measurement of student learning in MOOCs: An introduction to item response theory, scale linking, and score equating. Research & Practice in Assessment, 8(1), pp.26-39.

[3] Yong Chen, Wu He (2013). Security Risks and Protection in Online Learning: A Survey. The International Review of Research in Open and Distance Learning, Vol. 14, No 5, December 2013, pp.108-127 (http://www.irrodl.org/index.php/irrodl/article/viewFile/1632/2750)

[4] Garber, L. (2012). The Challenges of Securing the Virtualized Environment. Computer, January, pp.17-23.

[5] Social Media and Data Protection. Kinast & Partner (2014) (http://www.kinast-partner.com/data-protection-law/social-media-and-data-protection/)

[6] Weichert, T. (2013). Current Data Protection Challenges in Social Networks. Annual Conference on EU Data Protection Law 2013, 19 November 2013, Trier (https://www.datenschutzzentrum.de/vortraege/20131119-weichert-data-protection-social-networks.html)

[7] Romansky, R. (2012). Cloud Services: Challenges for Personal Data Protection. International Journal on Information Technologies and Security (ijits-bg.com), No 3, vol. 4, pp.67-80.

[8] Romansky, R. (2013). Distributed Information Servicing and Personal Data Protection. Bulgarian Science (in Bulgarian), No 59, pp.86-98 (http://image.nauka.bg/magazine/bg-science59.pdf).

[9] El-Khatib, K., L. Korba, Y. Xu, G. Yee (2003). Privacy and Security in E-Learning. International Journal of Distance Education Technology. Vol. 1, No. 4, October-December 2003, pp.1-19. Idea Group Publishing. NRC 45786 (http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.90.7927&rep=rep1&type=pdf)

[10] Hye-jin Kim (2013). E-learning Privacy and Security Requirements: Review. Journal of Security Engineering (ISSN: 1738-7531) Vol.10, No.5, pp.591-600 (http://www.sersc.org/journals/JSE/vol10_no5_2013/7.pdf)

[11] May, M., G. Fessakis, A. Dimitracopoulou, S. George (2012). A Study on User's Perception in E-learning Security and Privacy Issues, IEEE 8th International Conference on Advanced Learning Technologies (IEEE-ICALT 2012), Rome, Italy, 2012, pp. 88-89 (http://www.madethmay.com/images/2014/04/ICALT_2012_MMAY.pdf)

[12] Ahmad, A., M. Ahmed Elhossiny (2012). E-Learning and Security Threats. International Journal of Computer Science and Network Security, Vol. 12, No.4, April 2012, pp.15-18 (http://paper.ijcsns.org/07_book/201204/20120403.pdf)

[13] Diaz, V., J. Golas, S. Gautsch (2010). Privacy Considerations in Cloud-Based Teaching and Learning Environments. EDUCAUSE, November 2010, 10 p. (http://net.educause.edu/ir/library/pdf/ELI3024.pdf)

ABOUT THE AUTHOR

Prof. Radi Romansky, D.Sc., Department of Electronics, Computer Systems, and Technologies, College of Energy and Electronics at TU-Sofia, Professor on Informatics and IT in International Business School, Botevgrad, E-mail: rrom@tu-sofia.bg.

The paper has been reviewed.