Privacy Challenges when Implementing New Technologies in Education

Martin Zahariev[1]

University of Library Studies and Information Technologies, Republic of Bulgaria[1]

Abstract

In the world of today, the rapid technological advancement influences practically any sphere of public life. The education, a traditionally conservative system in Bulgaria, is no exception. Advanced technologies for video surveillance and algorithmic assessment of students become a reality rather than fiction. However, the usage of such technologies poses many challenges and even threats to the fundamental right to privacy of all participants in the educational process: students – who as per the European data protection legislation merit specific protection likely being less aware of the risks associated to the processing of their personal data; teachers; administrative staff working in the educational institution, etc. The present paper analyses some of the most common privacy issues that arise in the context of using ICT in the educational system. These include in particular: (i) the admissibility to install video surveillance and facial recognition systems for security and learning process control purposes in the school facilities; (ii) the legality of using automated tools such as algorithms and even artificial intelligence for assessing and evaluating students instead of a human teacher; (iii) the obligation to transparently inform the students as vulnerable persons about the processing of their personal data. The analysis is based on the Bulgarian and European court and administrative practice with particular emphasis on the opinions of the Bulgarian data protection supervisory authority – the Commission for Personal Data Protection. The conclusions made resemble the authors' experience as a practicing lawyer and as an academic researching from scientific point of view the problems of privacy and data protection in European Union (EU) law. Although focusing on the said problems from Bulgarian perspective, the paper can have practical implications and serve as a basis for future research in all EU countries which share the same data protection legal framework – Regulation 2016/679, better known as "GDPR".

Keywords: *Privacy, surveillance, recording, transparency, algorithms, assessment*

1. Introduction

Nowadays, the rapid technological advancement affects any sphere of public life. Information and communication technologies (ICT) are being increasingly applied in education, a traditionally conservative system in Bulgaria. Video surveillance and algorithmic assessment of students are becoming a reality rather than fiction. The usage of such technologies, however, poses many challenges and threats to the fundamental right to privacy of all participants involved in the educational process: students – who as per the EU General Data Protection Regulation (GDPR)[1] merit specific protection being less likely to be aware of the risks related to the processing of their personal data[2]; teachers; administrative staff, etc. This paper analyses how these privacy risks can be appropriately mitigated in compliance with GDPR – the new legislative standard in privacy which modern ICT-oriented education need to adhere to.

2. Video surveillance and facial recognition systems

The usage of video surveillance and facial recognition systems is widespread, including by small and medium enterprises. It comes as a no surprise that educational establishments (nurseries, kindergartens, schools and universities) also implement such systems for various purposes – protecting the life and health of students/teachers, securing the property, monitoring the learning process, establishing access control, etc. The easier it is to install a video surveillance system, however, the more complicated the privacy-related issues regarding its legality are.

In Bulgaria video surveillance in education should be assessed in the light of the general prohibition on following, photographing, filming, recording or being subject to any other similar activity without the individual's knowledge or despite his/her express disapproval, except when permitted by law (Art. 32(2) of the Constitution of the Republic of Bulgaria)[3]. In addition, the permissibility of CCTV surveillance/facial recognition systems in childcare and educational establishments was analyzed by the Commission for Personal Data Protection (the Commission) in two opinions.

According to Opinion Reg. No. П–5375/2017 of 30.04.2018[4], installation of cameras in these establishments can be deemed permissible for the purpose of improving the security and transparency of care, for resolving conflict situations in the process of upbringing children, as well as for protecting the life and health of the most vulnerable category of society as a whole – children and minor Bulgarian citizens. The Commission identified two possible legal grounds under GDPR for this type of data processing – vital interest (Art. 6(1)(d)) and public interest (Art. 6(1)(e)). However, the Commission set the boundaries to which the surveillance is proportionate, namely video surveillance was declared not permissible in dormitories, bathrooms, rest rooms and rooms for personal hygiene of children. According to the arguments set out in the opinion, by installing such devices in the said premises, children would be deprived of their the right to privacy and preservation of personal dignity and it would actually constitute a violation of the right to privacy. The Commission also emphasized the need to ensure transparency, more particularly by informing the parents/guardians and children about the video surveillance via warning signs containing details about the processing.
According to Opinion Reg. No. НДМСПО-17-916 of 21.12.2018[5], the installation of entrance-exit cameras for facial recognition connected to a school electronic diary for the purposes of automatic identification of students and recording absences in the diary violates the principles of lawfulness and proportionality of the processing. Considering the explicit disagreement of the parents, the Commission found that such processing can be considered not permissible automated individual decision making based on sensitive biometric data. The Commission prescribed that the regular school attendance control should be conducted via less privacy-intrusive measures.
Important conclusions regarding video surveillance in education can be drawn from the above practice. It is generally accepted that certain universal values such as protecting life and health, security and transparency of childcare deserve enhanced protection, including via privacy-sensitive measures like video surveillance. However, a careful case-by-case assessment is necessary on whether the processing is proportional and each time it is excessive, it should be reasonably restricted.

3. Algorithmic assessment of students without human intervention

The modern ICT computability capabilities make it possible to evaluate individuals, in the form of behavioral analysis/prediction, without human intervention. GDPR describes this type of data processing as “profiling” (Art. 4, 4))[6]. Furthermore, according to GDPR a machine (an algorithm, artificial intelligence, etc.) instead of human can theoretically make a decision, including based on profiling, that legally or similarly significantly affects an individual. This is qualified by GDPR (Art. 22) as an automated individual decision-making (AIDM)[7]. Such a scenario is possible in education as well where a school or university decides to implement evaluation techniques relying on automated processing only, i.e. where the assessment of students’ performance is fully automated. Although this approach seems to have certain advantages, such as ensuring equal treatment and eliminating the elements of subjectivity and prejudice, assessing students via AIDM poses threats to the fundamental rights and requires careful application in line with GDPR.
A general prohibition on AIDM is introduced by GDPR (Art. 22(1)). It might be lifted provided that one of the following exceptions is present (Art. 22(2)(a)-(c)):

- need to enter into/perform a contract with the data subject;
- authorization by EU/Member State law providing suitable safeguards for individuals;
- explicit consent.

Consent can be withdrawn at any time and is therefore inappropriate for student assessment purposes. The education is also a strictly state-regulated system where contract principles do not apply. Hence, the best approach is to regulate any AIDM in educational process by law on EU/Member State level. Any legislation authorizing AIDM in education should observe the minimum safeguards prescribed by GDPR (Art. 22(3)), namely the right of the affected individual (i) to obtain human intervention from the controller, (ii) to express own point of view and (iii) to contest the decision. This will mean that schools and universities applying AIDM need to ensure a human teacher for reviewing and, if necessary – for revising the respective assessment and for changing the student’s grade. Lastly, applying AIDM will most likely trigger additional GDPR obligations for the controller, including:

- conducting data protection impact assessment (Art. 35(3)(a)), and eventually – prior consultation with a data protection supervisory authority (Art. 36);

- obligation to appoint a data protection officer as the core activities of the controller would consist of processing which requires regular and systematic monitoring of data subjects on a large scale (Art. 37(1)(b)).

4. Transparency and right to information

Transparency being one of the foundations the EU legal system is based on is related to creating trust in the processes affecting the citizens by enabling them to understand, and if necessary, to challenge these processes[8]. GDPR envisages the transparency along with lawfulness and fairness as one of the main data processing principles (Art. 5(1)(a)) empowering individuals to hold data controllers and processors accountable and to exercise control over their personal data[8].

The most important manifestation of the transparency principle is the right of data subjects to receive and the correlative obligation of controllers to provide appropriate information about personal data processing. The content of this information is strictly prescribed by law (Art. 13-14 of GDPR) and includes practically all the important aspects of data processing – purposes, legal grounds for the processing, retention periods, data recipients, individuals' rights, etc.

In practice, the adherence to this legal requirement is ensured via a special document prepared by the controller (privacy policy, privacy notice, etc.) containing the relevant information. GDPR introduces multiple requirements on how this information should be presented for utilizing its usefulness for the ordinary citizen (Art. 12). In a nutshell, the information should be presented in a concise, transparent, intelligible and easily accessible form, using clear and plain language, thus avoiding any complex legal and IT jargons, in writing (or by other means, incl. electronically) and free of charge. A higher level of diligence is required when adapting this information for children which affects the educational process. As per the best EU practices, controllers informing children about the processing should *"ensure that the vocabulary, tone and style of the language used is appropriate to and resonates with children so that the child addressee of the information recognises that the message/ information is being directed at them"*[8]. The "UN Convention on the Rights of the Child in Child Friendly Language" is recommended as a good example for child-oriented language [8].

In that respect, kindergartens and schools should implement easily understandable privacy notices describing the data processing in the educational process and, if conducting video surveillance – place warning signs for it. A careful balance between the comprehensiveness and the intelligibility of the information needs to be achieved. To ensure accountability, reasonable solutions seem:

- to place the video surveillance warning signs at the entrances of the surveilled premises and in the security rooms of these facilities;
- to attach the privacy notices on paper at visible places (e.g. at the entrances, near the teacher/director department, at the bulletin board, etc.);
- to place this information on the institution's website – this should be only an additional channel for presenting the information, because not every student has access to a computer and the Internet. Therefore, it should not replace the paper-based approach for informing the students on premises.

5. Conclusion

New technologies create new opportunities – for society in general and for specific sectors such as education. The 21st century education is based on ICT, but the key to successful digitalization is adherence to the EU privacy standards. Ensuring data protection compliance in education is an interdisciplinary effort and requires cooperation from all the stakeholders – legal and IT experts, state bodies, teachers, educational institutions, parents, students. Only by combining the advantages of ICT and subjecting them to the rule of law can the ultimate purpose of education be achieved – to prepare the next generations for a better tomorrow.

References

[1] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF 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), OJ L 119/1 of 4.5.2016;

[2] Voigt, P., von dem Bussche, A., The EU General Data Protection Regulation (GDPR). A Practical Guide, Springer International Publishing AG, 2017, 383 pages, p. 21;

[3] Constitution of the Republic of Bulgaria, SG 56/13.07.1991, last amendment SG 100/18.12.2015;

[4] Opinion of the Commission for Personal Data Protection Reg. No. П–5375/2017 of 30.04.2018 regarding the introduction of video surveillance in childcare facilities (nurseries and kindergartens), as well as in schools,
URL: <https://www.cpdp.bg/index.php?p=element_view&aid=2106> (31.05.2020);
[5] Opinion of the Commission for Personal Data Protection Reg. No. НДМСПО-17-916 of 21.12.2018 regarding the installation of entrance and exit cameras for facial recognition related to a school electronic diary, URL: <https://www.cpdp.bg/?p=element_view&aid=2149> (31.05.2020);
[6] Zahariev, M., The evolution of EU data protection law on automated data profiling. // Privacy in Germany. Datenschutz and Compliance, Berlin, Erich Schmidt Verlag GmbH & Co. KG, 2017, N 02.17, pp. 73-79;
[7] WP29 Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, adopted on 3 October 2017, as last revised and adopted on 6 February 2018, WP251rev.01;
[8] WP29 Guidelines on transparency under Regulation 2016/679, adopted on 29 November 2017, as last revised and adopted on 11 April 2018, WP260rev.01.