Digital Citizenship and the Student's Digital Footprint: Questions of Application, Promotion and Data Protection

Iskandar Mukhametzyanov [a]
Institute for Strategy of Educational Development, Russian Academy of Education, Zhukovsky str. 16, Moscow, Russia

Keywords: Digital Citizenship, Student Digital Footprint, Student Data Protection.

Abstract: The digital transformation of the state also implies digital citizenship, and learning with the use of digital technologies leaves a "digital footprint" of the student on the Internet. During the period of self-isolation caused by the COVID-19 pandemic, the problem of data protection of education participants has significantly worsened. For the purposes of this study, we have reviewed the literature of recent years, reflecting the results of various studies, including national ones, focused primarily on identifying the conditions for the implementation of "digital citizenship" and the reasons for the decline in the quality of education, combined with the problems of protection of students' personal data. "Digital citizenship" is a set of competencies of a citizen and the actions of the state in ensuring equal access to digital information and the protection of citizens in digital communication. The implementation of distance learning in the period of COVID-19 revealed the problems of inequality of students in terms of access to information, as well as the lack of digital competencies in learning and ensuring its security, the weak readiness of "digital citizens" to effective use of their digital citizenship.

1 INTRODUCTION

The digital transformation of the state also implies digital citizenship. Learning with the use of digital technologies leaves a "digital footprint" of the student on the Internet. During the period of self-isolation caused by the COVID-19 pandemic and the forced use of commercial and adapted communication platforms, the problem of data protection of education participants has significantly worsened. And without the formation of competencies not only in terms of citizenship of the student, but also in terms of the protection of such communication and personal data, digital citizenship is impossible.

2 RESEARCH METHODS

For the purposes of this study, we have reviewed the literature of recent years, reflecting the results of various studies, including national ones, focused primarily on identifying the reasons for the decline in the quality of education and the depressing situation with the protection of personal data and "digital traces" of students.

3 DISCUSSION

Digital citizenship (DS) is the responsible use of information and communication technologies by a person to interact with their community. The peculiarity of the existence of this concept is its dependence on the availability of access to digital technologies. In total, there are nine main technologies, the totality of which determines the presence of DS, partial or complete. These are: digital access, digital communication, digital commerce, digital literacy, digital ethics, digital law (responsibility for actions on the Internet), digital rights and duties, digital health (physical and psychological well-being in the digital world) and digital security (including cybersecurity with the protection of personal data (The Nine Elements of Digital Citizenship, 2016). As the experience of the

[a] https://orcid.org/0000-0000-0000-0000

Mukhametzyanov, I.
Digital Citizenship and the Student's Digital Footprint: Questions of Application, Promotion and Data Protection.
DOI: 10.5220/0010616600003170
In *Proceedings of the International Scientific and Practical Conference on Computer and Information Security (INFSEC 2021)*, pages 12-16
ISBN: 978-989-758-531-9; ISSN: 2184-9862

COVID-19 pandemic has shown, not all people in the world have digital access, and its quality often simply does not allow them to conduct any activities in a digital format. Accordingly, when talking about the "digital inequality" of citizens in access to technology, it is necessary to proceed from the understanding of "digital citizenship" as a feature of the organization of the state and self-organization of citizens in the first place, and as a manifestation of human activity in the second place (Mossberger & Tolbert, 2021). Initially, human activity on the Internet could have an anonymous nature, since it did not provide for a significant "digital footprint". With the development of information and communication technologies and their penetration into all aspects of human life, there is less and less opportunity for anonymity, and because of the use of social networks and tracking of network addresses of access devices and other traces of human activity people can already forget about anonymity. And in this regard, it is necessary to educate a person not just about their citizenship, but also their digital citizenship, since their virtual copy, to one degree or another, is an integral part of the person themselves. The concept of digital citizenship is inextricably linked to digital literacy and digital rights. However, they did not develop at the same time, digital literacy became formalized as digital citizenship, but without digital law it has no legitimation in the conditions of modern society (Pangrazio and Sefton-Green, 2021).

At present, the DS is an informal concept and can have both negative and positive interpretations based on the goals and results of using digital tools. The intermediate stage of this activity is creation of the "digital footprints". The DS is formed in the process of learning skills and techniques of performing activities in the digital environment. In these conditions, parents and teachers have a significant influence on the formation of the DS. The cause of a negative impact on a child can be a situation of cyberbullying and knowledge of the rules of digital citizenship can help prevent it. Knowing how to properly use modern technology can help prevent technology addiction and its associated health consequences. In this regard, special importance is attached to communication between the teacher and the student's parents, teaching the student the rules of activity in the digital environment, protecting personal information, and handling the "digital footprint".

3.1 The "digital footprint". Concept and Classification

The digital transformation of education with the implementation of educational interaction in a digital format implies the use of the "digital footprint" (DF) of the student for educational purposes. In the broadest possible sense, a DF is a trace of a person's online activity and nothing more. In the scope of this work, these are traces of online activity, that was done for educational purposes. Quite conditionally, the DF can be divided into positive and negative, active and passive, formalized and unformalized, open and hidden.

When talking about the active and passive DF, it is necessary to talk about information, including that about a person, posted in any way on the Internet consciously. In the case of passive information, it is secondarily placed, indirectly touching a particular phenomenon or person. Today, an extremely large amount of information is posted on the Internet and we are no longer interested in the fact of its existence, but in the fact and ways of its transformation for the purposes of a particular person or subject of human relations. The sequences of actions, the logic of decision-making, forecasting of results, risk assessment in the use of information become topics of interest. As a result, the digital footprint allows people to create a psychological portrait of a person and predict a variety of aspects of their behaviour. An active form of forecasting can be providing a person with information and evaluating their actions based on their previous DF. In the passive form, the assessment of any actions in a changing environment takes place. This allows for evaluation and prediction of actions in extreme conditions.

The positive and negative aspects contain a representation of the information by the person themselves. It is placed by them consciously, in order to publicly demonstrate certain aspects of their activities. If it is placed by someone in order to discredit the person, while having their own DF (explicit or hidden), then it has a negative character.

If information or activity is posted or implemented under a specific name, it is explicit. Data or news can be posted or used under fictitious names and respectively are hidden in nature.

Formalized information is usually placed in the format of positive information, such as a portfolio or resume. Unformalized information is placed without a specific structure and can be either positive or negative.

3.2 Positive and Negative Aspects of the Digital Footprint

The specifics of human behaviour patterns in communications, in certain actions, in behaviour in society and preferences show the personality characteristics of each person. Considering them, based on their DF, it is possible to predict the actions of a person in a certain situation with a high degree of probability. Thus, if this happens without the knowledge of the person, there is a violation of their privacy and the data obtained can be used for illegal purposes. It is possible to model a situation in which the actions of the subject can be destructive or self-destructive, but the inevitability of these actions, even for the object of manipulation themselves, is due to all their previous experience. An example is the destructive network communities, when the very inclusion of a person in its composition already shows readiness for certain actions.

Speaking about the positive orientation of the DF, we can talk about prediction, for example, of the student's learning behaviour (Azcona, Hsiao & Smeaton, 2019). At the system level, the use of the DF allows us to implement continuity and integration of educational levels, effectively organize and manage the educational process, and the most popular direction at the present time, manage the educational system (Mantulenko, 2021). When evaluating the formal data of the intermediate and final educational assessments and analysing the methods used to solve the task based on the DF, the teacher gets the opportunity to objectively evaluate the students' understanding of certain subject areas. On the basis of this, they can either provide the student with a different way to solve the task, or change the task itself, break it into stages, which ultimately will allow individualizing learning using positive and objective feedback. It is also possible to stimulate the student by using the methods and areas of activity that are most preferable for them in order to create positive DF for them as an aspect of subsequent effective employment (Buchanan, Southgate, Scevak & Smith, 2018; 12 Reasons to Research a Job Applicant's 'Digital Footprint', 2021). There is no doubt that the COVID-19 pandemic period has changed all students in one form or another. Without a choice, they had to learn with the use of digital technologies that change the traditional way of the education system, change the priorities in education, change the systems of assessing the quality of educational activities, but one thing is certain, that this change can no longer be reversed (Nordmann et al., 2020). It should be remembered that the activities of the student and teacher within the framework of the DL have a certain "digital footprint" that requires attention in terms of data protection and privacy (Zwitter, 2014). Particular importance should be attached to this based on the possibility of analysis of the DF with the use of artificial intelligence and creation of a psychological portrait of a person, possible reactions in a changing environment and possible psychiatric problems. Which, in the end, provides the possibility of manipulating a person (Bidargaddi et al., 2017). Mass distance education during the COVID-19 pandemic was in itself a significant stress factor for the mental health of students at all levels of education. According to studies of more than 1.2 million children and adolescents, based on self-reports, 10.5% said that they had signs of psychological distress (Qin et al, 2021).

3.3 Digital Footprint Management and Personal Data Protection

The very existence of DF has both a negative and a positive assessment. At present, in the conditions of an extremely weak level of knowledge in terms of information protection, the negative aspect of its use dominates. In these conditions, the formation of skills of maintaining confidentiality of activity on the Internet and the removal of data of the DF, the knowledge of the possibility of their illegal use is not only important for ensuring a comfortable life for a person, but also for ensuring its security. In relation to the education system, the accumulation of the student's DF in the information systems of the educational organization (EO) and the prediction of their educational activities based on their DF and real behaviour allow the EO to form a personal educational database. There is no doubt that this process should be based on the informed consent of the student, both regarding the process as a whole and collection of specific data groups (Jones, 2019).

The basis for the protection of personal data are the national acts in this field. In Russia, these are Federal Law No. 152-FZ from 27.07.2006 "On Personal Data", Federal Law No. 436-FZ from 29 December 2010 "On the Protection of children from information that harms their health and development" and a number of other legislative acts. But the presence of these regulations does not ensure the effectiveness of their application, first of all, because of their extremely inactive popularization in the education system for individuals, the main consumers of digital content. An example of specialized regulations is the California's SOPIPA (Student Online Personal Information Protection Act, 2014),

which prohibits companies from using student's personal data obtained as a result of educational activities on the Internet and using educational platforms, transferring it to third parties and using it for personalized advertising. When using educational platforms and applications by persons under 13 years of age, it is mandatory to have informed parental consent. The communication platforms used during the pandemic (Zoom and others) fall under the scope of this law when used for training purposes. At the same time, showing the screen to third parties outside the classroom and teacher community is a disclosure and distribution of personal data. And in many ways, the security of the students' DF in this case is assigned to the administrator of a particular conference, since only they determine the authority and level of access to the personal data of all participants. Based on this, the level of competence in this area of the teacher when using any communication platforms and applications in distance learning should not only be formed, but also certified by the relevant services in the field of information security.

At the same time, it is noted that popular educational platforms do not protect the data of children in distance learning, and there are 1.6 billion children worldwide. Permission to use those platforms for educational purposes does not contain guarantees of information security. Fifty-eight percent of them are highly risky when ensuring the digital privacy of children. A third of the platforms had security issues, including the use of software with known vulnerabilities and insecure Internet cookies, while three quarters contained ad tracking, including sharing information with Facebook and Google ("Lockdown Learning Platforms "Put Children's Privacy at Risk", 2020).

A special case in terms of data protection and illegal use of the DF of any participant in the communication is the use by students of personal or work devices for Internet access of their parents for educational purposes. This allows attackers to gain access to the personal and commercial information of students' parents through virtually unprotected educational communications. A large number of applications from the period of 2020 in the area of online commerce and home delivery of goods practically do not provide data protection. A 2019 study of students in grades 3-8 shows that they most often use the same password for most applications and programs on the Internet (58% of students in grades 3-5 and 78% of students in grades 6-8). More often, they have one or two passwords for school activities and three or four passwords for home activities. Most common are passwords with an average length of 7 (grades 3-5) and 10 (grades 6-8) characters of weak and medium reliability, and only 13% of children have strong passwords. This is due to the weak development of cognitive and linguistic abilities. And training in this area should be aimed both at creating effective and reliable passwords, as well as at learning secure ways to store them (Choong, Theofanos, Renaud and Prior, 2019).

4 CONCLUSIONS

The provisions on digital citizenship and the student's digital footprint that are considered in this paper are inextricably linked with the concept of digital communication, i.e. interpersonal communication with the use of information and communication technologies. The use of technologies for educational purposes allows to remove a significant amount of organizational and managerial problems from the organizers of education. This was demonstrated during lockdown and distance learning during the pandemic. The difficulties of this period were both informational in terms of the content of education in digital form, and communicational – in regards to the use of open communication platforms. And this has led to both an unusually large increase in the digital footprint of all participants in the learning process, and a significant reduction in data privacy. Both, in essence, are components of effective digital citizenship, not declared, but real. Even with the end of the pandemic, digital learning will remain as a component of blended learning, and it is in the digital part of it that the "Achilles' heel" of digital citizenship remains. It is the unwillingness and inability to implement all the elements of citizenship in an environment, that is safe for a person, to protect the "digital footprint" of the student and teacher, to individualize learning based on the analysis of the "digital footprint". The pandemic has shown that no educational system in the world has paid due attention to the component of blended learning at the student's place of residence. There is no regulation of the organization and management of educational activities of students at their place of residence, and there is no coordinated activity of the educational organization and the student's parents in ensuring the security of education and data protection. There is no doubt that all educational programs at all levels of education should include these components, since now they will determine not only the child's ability to learn, but also their ability to become a citizen.

REFERENCES

12 Reasons to Research a Job Applicant's 'Digital Footprint' (2021, February 4). Retrieved February 8, 2021 from: https://www.forbes.com/sites/forbescoachescouncil/2021/02/04/12-reasons-to-research-a-job-applicants-digital-footprint/?sh=41d795117259

Azcona, D., Hsiao, I. H. & Smeaton, A.F. (2019). Detecting students-at-risk in computer programming classes with learning analytics from students' digital footprints. User Model User-Adap Inter 29, 759–788. https://doi.org/10.1007/s11257-019-09234-7

Bidargaddi, N; Musiat, P; Makinen, V-P; Ermes, M; Schrader, G; Licinio, J (2017). Digital footprints: facilitating large-scale environmental psychiatric research in naturalistic settings through data from everyday technologies. Molecular Psychiatry, 22(2), 164–169. doi:10.1038/mp.2016.224

Buchanan, R., Southgate, E., Scevak, J., & Smith, S. P. (2018), 'Expert insights into education for positive digital footprint development', Scan, 37(2). Retrieved February 20, 2021 from: https://education.nsw.gov.au/teaching-and-learning/professional-learning/scan/past-issues/vol-37-2018/expert-insights-into-education-for-positive-digital-footprint-development

Choong Y., Theofanos M.F., Renaud K., Prior S., (2019) "Passwords protect my stuff"—a study of children's password practices, Journal of Cybersecurity, Volume 5, Issue 1, tyz015, https://doi.org/10.1093/cybsec/tyz015

Jones, K.M.L. (2019). Learning analytics and higher education: a proposed model for establishing informed consent mechanisms to promote student privacy and autonomy. Int J Educ Technol High Educ 16, 24 https://doi.org/10.1186/s41239-019-0155-0

Lockdown Learning Platforms "Put Children's Privacy at Risk". (2020, September 22) Retrieved February 20, 2021 from: https://www.forbes.com/sites/nickmorrison/2020/09/22/lockdown-learning-platforms-put-childrens-privacy-at-risk/?sh=3148620f12c8

Mantulenko, V.V. (2021) Prospects of Digital Footprints Use in the Higher Education. In: Ashmarina S., Mantulenko V. (eds) Current Achievements, Challenges and Digital Chances of Knowledge Based Economy. Lecture Notes in Networks and Systems, vol 133. Springer, Cham. https://doi.org/10.1007/978-3-030-47458-4_67

Mossberger, K., and Tolbert, C. J. (2021). Digital Citizenship and Digital Communities: How Technology Matters for Individuals and Communities. International Journal of E-Planning Research (IJEPR), 10(3), 19-34. doi: 10.4018/IJEPR.20210701.oa2

Nordmann E, Horlin C, Hutchison J, Murray J-A, Robson L, Seery MK, et al. (2020) Ten simple rules for supporting a temporary online pivot in higher education. PLoS Comput Biol 16(10): e1008242. https://doi.org/10.1371/journal.pcbi.1008242

Pangrazio, L., & Sefton-Green, J. (2021). Digital Rights, Digital Citizenship and Digital Literacy: What's the Difference? Journal of New Approaches in Educational Research, 10(1), 15-27. doi: http://dx.doi.org/10.7821/naer.2021.1.616

Qin Z, Shi L, Xue Y, et al. (2021) Prevalence and Risk Factors Associated with Self-reported Psychological Distress Among Children and Adolescents During the COVID-19 Pandemic in China. JAMA Netw Open.; 4(1): e2035487. doi:10.1001/jamanetworkopen.2020.35487

Student Online Personal Information Protection Act (2014, September 29). Retrieved February 20, 2021 from: https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201320140SB1177

The Nine Elements of Digital Citizenship. (2016, December 14). Retrieved February 20, 2021 from: https://milunesco.unaoc.org/mil-resources/the-nine-elements-of-digital-citizenship/

Zwitter, A. (2014) Big data ethics. Big Data Soc 1(2):2053951714559253. https://doi.org/10.1177/2053951714559253