DIGITAL MINDSET IN EDUCATION – SECURITY EDUCATION –

Andreea LOSEKAMM

Management Expert, US Department of State, General Consulate in Frankfurt, Germany

10.55535/RMT.2023.2.10

Safety and the protection of freedoms constitute key challenges the education system is currently facing in the context of digitalization, challenges that require the promotion of a more elaborate definition of digital democracy correlated with concerns related to human rights, development inequality depending on access to education, responsibility and, last but not least, building consensus in highly diverse environments. Therefore, security as a fundamental value of democratic societies requires a reassessment in relation to the principles promoted by political institutions – inclusion, responsibility and transparency –, debatable against the background of political polarization and the emergence of new digital technologies. The present article is not intended to formulate a general theory on how the digitalization of education and democracy relate or are mutually exclusive. It deals with more or less contingent situations and raises additional – including empirical – questions about the role that digitalization in the education system can have for the state of democracy, regardless of the level of understanding. The intent is directed to the concrete mode in which digitalization can be beneficial or inadequate for democracy, contributing to a better understanding of the challenges. The reader can translate it into own environment, linking personal reading to specific democratic processes, including the level and type of digital activity.

Keywords: education system; digitalization; cyber security; democracy; critical infrastructures;

ROMANIAN MILITARY THINKING

DEVELOPMENT EXPLAINED IN BINARY NUMERIC CODES

The digital world is divided into clear, secure and rational structures, consisting of series of sequences of numbers – finally binary numeric codes. Digitalization itself is basically nothing more than the representation and storage of information, which results in the expression of actions and values in codes. However, the impact of digital transformation is not simplified by bringing it to a common denominator. The main values of democracy – freedom, equality, dignity, solidarity, the rule of law – cannot be transposed into numerological sequences. In the form of codes, they are equally applicable to both physical and virtual reality, and the measures to be implemented in the field of cybersecurity must fully comply with these principles.

The reconfiguration of the relationship between security and democracy is a priority in the national efforts to stabilize the democratic crisis in the education system invoked by the inability of some governments to provide a responsible and adaptive system in line with digital transformation. The study of safe and adaptive digitalization varies, but does not go beyond the concept of regionalism or globalization, since inclusion is essentially due to these concepts. In understanding the perceptions of security towards the complexity of the technological process, it is necessary to examine this fundamental reconfiguration over two distinct perspectives: the readjustment and redesign of (democratic) security, encompassing the different and sometimes contradictory ways in which democratic forms of security governance change.

The study of safe and adaptive digitalization varies, but does not go beyond the concept of regionalism or globalization, since inclusion is essentially due to these concepts. In understanding the perceptions of security towards the complexity of the technological process, it is necessary to examine this fundamental reconfiguration over two distinct perspectives: the readjustment and redesign of (democratic) security, encompassing the different and sometimes contradictory ways in which democratic forms of security governance change.

EDUCATION – DEMOCRACY – SECURITY BALANCE

The topic of digital democratization is a complex one, related to different concepts such as security, participation, adaptation and last but not least transformation. Starting from these principles, the article offers a concept of digital democracy as a combination of dimensions: information – participation – transformation, dimensions taken from the foundation of education.

Education is a basic need for every human being, and digital education is the current trend and necessity. Not unpredictable at all, this topic is often addressed in connection with data processing and involves concerns about privacy, increasing inequality, risk of stigmatization and discrimination (whether it is deliberate or simply an unintentional consequence). Given the enormous costs of creating and maintaining courses on online platforms, it is surprising that security is not yet considered a major problem by the authorities, including teachers and students. Unlike traditional research in the field of security, which has largely been determined by military requirements to impose secrecy, in the field of e-learning it is not the information itself that must be protected against unauthorized access, but the way in which it is presented. In most cases, the knowledge contained in e-learning programmes is more or less accessible; therefore, it is not the information itself that is the destabilizing element of security, but the way used to transmit it.

Unlike traditional research in the field of security, which has largely been determined by military requirements to impose secrecy, in the field of e-learning it is not the information itself that must be protected against unauthorized access, but the way in which it is presented. In most cases, the knowledge contained in e-learning programmes is more or less accessible; therefore, it is not the information itself that is the destabilizing element of security, but the way used to transmit it.

In a secure learning environment, users should not be worried about the threats specific to learning platforms and electronic communication in general. A secure learning platform should incorporate aspects of security so that most processes can be transparent to the teacher and the student. However, ensuring a completely secure system is a too ambitious goal, because nothing can ever be completely secure and – at the same time – still remains usable. Therefore, the system should allow the user to decide upon the compromise between utility and security.

INFORMATION SECURITY VULNERABILITIES

For the development of operational plans, the combination of threats, vulnerabilities and their effects must be assessed in order to identify important trends and decide whether efforts should be made to eliminate or reduce threat and vulnerability capabilities and to assess, coordinate and eliminate conflicts of all cyberspace operations (Locke, Gallagher, 2011, p. 1).

Looking at the democratic system from the perspective of increasing vulnerabilities, we find that the new security model must be – today more than ever – responsive to global challenges and able to cope with an increasingly complex and digital political environment. The rise in populism, increasingly radical mentalities, declining trust in political institutions and increased expectations of political participation add additional challenges to the established processes and structures of liberal democracies. While digital transformation will not be the only answer to these challenges, it will be the key for democratic institutions and political stakeholders to act decisively in an increasingly innovative world.

The current context displays a large array of examples of resistance to innovation or differential adaptation of new technologies (Frey, 2019, p. 59). The personalization of a social system is not done by itself. Participation must be personalized; each group requires a different approach, a different language and a different working method (European Union Agency for Network and Information Security/ENISA, 2015). The opportunities that digitalization offers for democratization are far from being fully exploited because technological change is a profound change: an often contested political process, the outcome of which depends not only on the technologies themselves, but also on how countries react to them (Schaefer, Coopersmith, 2018).

The opportunities that digitalization offers for democratization are far from being fully exploited because technological change is a profound change: an often contested political process, the outcome of which depends not only on the technologies themselves, but also on how countries react to them.

From the perspective of the political sphere, digitalization is seen mainly as a threat to democratic discourse and not as an opportunity. Bogdan Aurescu himself, in his capacity as Minister of Foreign Affairs, declared on the occasion of the celebration of the International Day of Democracy (2021) that the threats to democratic regimes have transcended the borders of a physical nature, spreading in the virtual world (*Bursa*, 2021).

A state must develop a comprehensive information security policy that encompasses all the necessary areas and critical cybersecurity functions within the institutions. The focus of policy documentation must be technical, physical, and administrative.

NOTIONS AND CONCEPTS OF INFORMATION SECURITY

The notion of IT or cyber security is defined as *"the state of normality resulting from the application of a set of proactive and reactive measures ensuring the confidentiality, integrity, availability, authenticity and non-re-confirmation of electronic information, public or private resources and services in cyberspace"* (ENISA, 2022). Information security is the protection of information against threats, implemented to ensure the continuity of the information flow. The Cyber Security Challenge Germany/CSCG recommended, in 2015,

that the European Commission should harmonize the use of the key terms *"cybersecurity", "NIS"* and *"cybercrime"* across the EU, based on existing definitions. Currently, official communications use all three terms without distinction between them, which risks being interpreted differently in different EU Member States (or languages). The CSCG also recommended the establishment and implementation of an appropriate governance model for the three areas, with a particular focus on avoiding *"silo work"*[1] on topics that are inherently associated (CNRISC, 2018).

By restricting the general context of discussions on cybersecurity at national level, we note the importance of conceptually separating the main directions of action: cyber defence, cybercrime, national security, critical infrastructures and emergency situations, international cyber diplomacy and Internet governance. There is a need to set out very clearly the roles and levels of accountability for each responsible individual national institution.

Information security governance is defined as "establishing and maintaining the control environment for managing risks related to the confidentiality, integrity and availability of information to support processes and systems".

According to ISO (ISO 38500[2]), governance specifies the accountability framework and provides oversight to ensure that risks are adequately mitigated while management ensures that controls are in place to mitigate risks. Management recommends security strategies. Governance ensures that security strategies are aligned with business goals and compliant with regulations. Information security governance is defined as *"establishing and maintaining the control environment for managing risks related to the confidentiality, integrity and availability of information to support processes and systems"* (Moulton, Coles, 2003, pp. 580-594). From another point of view, it is considered an integral part of governance that involves the implementation of governance concepts and principles regarding information security issues (Abu-Musa, 2010, pp. 226-276). Information security governance,

[1] *"Silo work"* means operating in a kind of bubble – on your own or as part of an insular team or department. Although the historical definition of a silo is a container (traditionally used on farms for storing grain or cattle food), the word also has a more abstract meaning today. It is often employed as a metaphor for groups of people (e.g., a team is a *"container"* of colleagues) who work independently from other groups. According to Dr. Gillian Tett, an anthropologist turned financial journalist, *"silos are cultural phenomena, which arise out of the systems we use to classify and organize the world"*, https://www.ideagen.com/thought-leadership/blog/working-in-silos", retrieved on 11 February 2023 (ed. note) .

[2] ISO/IEC 38500:2015 – *Information technology. Governance of IT for the organization* – applies to the governance of the organization's current and future use of IT including management processes and decisions related to the current and future use of IT, https://www.iso.org/standard/62816.html, retrieved on 28 February 2023 (ed. note).

in essence, encompasses good risk management, robust reporting control, testing, training and last but not least constant responsibility. It provides strategic direction for cybersecurity activities and ensures the achievement of nationally established cybersecurity objectives.

A good process of governing information security can transform an institution and generate one or more of the following cybersecurity benefits: (1) structured, focused, and prioritized allocation of time, economic resources and efforts; (2) compliance with information security policies; (3) better predictability and less uncertainty; (4) decision-making that is based on a clear structure; (5) a consolidated position when faced with legal consequences; (6) clear responsibility of the actors involved and better protection of information.

In order to help implement good information security governance, a robust core framework is essential to support and associate perfectly with the objectives of democracy. A cybersecurity framework gives states the ability to protect themselves from evolving cyber threats. The main objective of a cybersecurity framework includes: (1) harmonizing cybersecurity approaches and creating a common language; (2) setting the optimal level of cybersecurity adapted to the environment and specific needs; (3) allocating a sufficient cybersecurity budget for the implementation of the framework; (4) efficient exchange of knowledge about cyber risks.

According to the National Institute of Standards and Technology (NIST), information security governance involves establishing and maintaining a framework that provides assurance that information security strategies are aligned and support governance objectives, are consistent with applicable laws and regulations by complying with internal policies and policies, and controls and provides responsibility sharing, all in an effort to manage risk. This framework comprises five elements: it identifies, protects, detects, responds, recovers.

The structure of the simplified security concept has three levels (Tîrziu, 2015, pp. 121-122): (1) Physical security consisting in preventing, detecting and limiting direct access to information. At the moment, information destruction due to the vulnerability of the physical security level is considered to represent the greatest vulnerability. (2) Logical security represented by the totality of the methods that ensure the control over the access to the resources and services of the system.

A good process of governing information security can transform an institution and generate one or more of the following cybersecurity benefits: structured, focused, and prioritized allocation of time, economic resources and efforts; compliance with information security policies; better predictability and less uncertainty; decision-making that is based on a clear structure; a consolidated position when faced with legal consequences; clear responsibility of the actors involved and better protection of information.

(3) Legal certainty is the level constituted by a collection of national laws intended to regulate the act of violating the first two levels of security mentioned above and to establish criminal sanctions for those acts (Locke, Gallagher, p. 1).

TECHNOLOGICAL SETTING IN ROMANIAN EDUCATION

The objectives of e-learning are concerned with providing hybrid teaching on a large scale, and the main goal in close connection with security is to ensure the availability and integrity of information. E-learning is the implementation of technology to support the learning process, through which knowledge or information can be accessed using communication technology. The learning process can be continuous, provided that the availability of the content exists online. Although the long-term consequences of economic, social and political developments are too unpredictable, a speculative topic, the first effects of the technological setting on the Romanian educational landscape have been noticeable for some time. Society, culture and education are equally augmented and affected by the ongoing digitalization, thus having a bivalent influence on the development of knowledge and political and social structures participation.

E-learning is the implementation of technology to support the learning process, through which knowledge or information can be accessed using communication technology. The learning process can be continuous, provided that the availability of the content exists online.

The year 2020 marked the beginning of the pandemic of the Sars-COV-2 virus and the disease associated with Covid-19. At the same time, the need to reconfigure the approach practices in the education system was brought to the fore, through: lack of predictability; a heterogeneous school network with a strong digital divide between schools; insufficiently developed digital skills for the efficient organization of the teaching process in the online environment; reduced access to technology and reduced internet connectivity; reduced possibilities for families to provide support to beneficiaries of education, children, for participation in online lessons (Smart-Edu, 2020). The abrupt shift from traditional face-to-face interaction to the online environment soon showed that the future of education involves emerging technology and that teaching, learning and digitalization cannot be discussed disparately. In this context, the education system has undergone revolutionary changes, using the Darwinian phrase *"neither the strongest species, nor the most intelligent, but the most easily adaptable will survive"*.

However, a standard digitalization strategy has not yet been developed. The fundamental approach lies in identifying solutions for the transfer of knowledge at a global level; and adaptive methods geared towards uniform inclusion. The transfer of practices and methods between institutions at any level is considered a complex problem that requires the engagement of all resources. Understanding this transfer provides a necessary and sufficient foundation in managing development as it can support complex management systems to become innovative and build dynamic capabilities. The transfer of other models of knowledge management is therefore imperative for addressing topics such as anticipation systems, for assessing the risks to the security of using the technology with and for students.

In relation to the diffusion of the social security culture, the emergence of digital democratisation practices and models calls for emerging and integrable transparency for the stages of institutional adaptation. Next, such a solution involves both adapting the legislation (adapting the security and information environment) and a well-defined strategy (adapting the security and information organization).

MAIN CHALLENGES, PRIORITIES AND COURSES OF ACTION

The improvement of software products, their availability and the education system in the field of introduction and use of information technology is thus a dominant feature in the development of the management (but also of other) current processes.

The **key challenges** therefore remain the same: accessibility, inclusion, the acquisition of digital skills and, last but not least, security for all actors involved. The most important position remains that of the human being. The improvement of software products, their availability and the education system in the field of introduction and use of information technology is thus a dominant feature in the development of the management (but also of other) current processes. Therefore, how can the Romanian education system cope with the security risks related to the digital revolution without jeopardizing the fundamental democratic values? How inclusive is the security and cooperation dialogue at the governmental and institutional level? And finally, what are the mechanisms by which a responsible digitalization is being reconstructed?

The most common solution in such contexts is the forced development of new perspectives. The source of this paradox derives from the concept of digital democracy as a combination of dimensions: information, security, participation, and transformation. The call

is made towards an image of digitalization as a process that goes beyond previous analogical processes, presenting alternative paths to implementing and seizing the opportunities of responsible digital democracy by readjusting and redesigning mechanisms. Starting from the patterns of interaction between the Romanian educational institutions and the learning environment at international level, the paper proposes as a sustainable solution to innovation the idea of defining the governance of information security.

A new theoretical perspective that drifts into an adaptive strategy of knowledge management, without excluding the risks involved, is required. Adapting complex systems to shape themselves to current models imperatively requires an adaptive plan. The method will determine which structure within this equation is subject to change and what structural strategies need to be applied so that the structure and the whole system can fit better into the social environment. The plan aims to create such new directions aimed at improving the performance of participatory resources and eliminating threats to the democracies under review.

The use of technology in education is not only a trend or an influence on educational processes. In the current circumstances, the approach is a necessity for shaping the future of students by acquiring specific capabilities and skills.

Priorities and courses of action. One can say that the use of technology in education is not only a trend or an influence on educational processes. In the current circumstances, the approach is a necessity for shaping the future of students by acquiring specific capabilities and skills. In anticipation for this need to respond punctually to the challenges listed above, the clear identification of priorities is a must. Only in this way can directions of action be anchored in initiatives, measures and programmes that support the role of digital technology in the development of education and training systems.

Smart Edu for Modern, Accessible School, based on Digital Resources and Technologies, inspired by the Strategy on the digitalization of education in Romania proposes the following priorities: accessibility, connectivity, community, digital educational ecosystem, innovation, sustainability (Smart-Edu, 2020).

Such an approach is required to be correlated with the stage of implementing an action plan and, most likely, coincides with the preparation stage of the normative and legislative framework that supports the responsible and safe digitalization in the Romanian education.

CONCLUSIONS

In this article, information about technology and security in the education system has been presented in terms of a research agenda. We have highlighted that the security of the education institution requires a substantial contribution to research and development activities. The interactive reconfiguration of the technical and social infrastructures of the contemporary society, examined in their socio-technical educational context, comes in line with the dynamics of evolutions and trends at global level: information, the most important resource.

Security behaviour is correlated with the use of technology and the culture of information security in schools. In educational environments, the problem of user security behaviour is seen as a multidimensional phenomenon combined with the use of technology, learning, communication and teaching. Thus, theoretical commitments to understanding the culture of information security should be analysed based on concrete practices and interactions during the use of e-learning. Awareness of information security is of paramount importance, because it can help us identify potential threats before they occur and at the same time apply measures to support responsible and secure digitalization over time. Referring to Romania's objectives in the process of developing information education and implementing electronic education programmes, it is found that steps are still needed to ensure all resources and an integrated framework for access to a quality education in the digital age. The development of a national programme based on the milestones drawn by the Strategy on the digitalization of education in Romania meant to ensure the elaboration and implementation of concrete cyber security projects is a priority.

Referring to Romania's objectives in the process of developing information education and implementing electronic education programmes, it is found that steps are still needed to ensure all resources and an integrated framework for access to a quality education in the digital age.

The lack of a unitary approach to initiatives, measures and programmes aligned with the current context of information security issues represents a risk factor for ensuring the confidentiality of information and the security of the components of the information system of the institutions. Compromising information security can lead to damaging the credibility of the public institution, as well as to fraud or data destruction, disclosure of confidential information etc. The phenomenon of cybercrime is, by its nature, rapidly developing, transnationally, thus without borders. Depending on the type of vulnerability, the protection methods specific to today's information

technology are varied. The solutions given by the courses of action represent only the start in achieving more and more elaborate, performant security standards and technologies, making it increasingly difficult to exploit the vulnerabilities of a technological nature.

BIBLIOGRAPHY:

1. Abu-Musa, A. (2010). *Information Security Governance in Saudi Organizations: an Empirical Study*. In *Information Management & Computer Security*, 18(4), pp. 226-276.
2. Aurescu, B. (15 September 2021). *"Amenințările la adresa regimurilor democratice au depășit granițele de natură fizică, răspândindu-se în lumea virtuală" (Threats to democratic regimes go beyond the physical world, being present in digital world too).* In *Bursa*, https://www.bursa.ro/bogdan-aurescu-amenintarile-la-adresa-regimurilor-democratice-au-depasit-granitele-de-natura-fizica-raspandindu-se-in-lumea-virtuala-07992445, retrieved on 24 November 2022.
3. Frey, C.B. (2019). *The Technology Trap: Capital, Labor, and Power in the Age of Automation*. Princeton, NJ & Oxford: Princeton University Press.
4. Locke, G., Gallagher, P.D. (March 2011). *Information Security*. *NIST Special Publication* 800-39, Gaithersburg, MD: Computer Security Division/Information Technology Laboratory/National Institute of Standards and Technology.
5. Moulton, R., Coles, R.S. (2003). *Applying Information Security Governance*. *Computers & Security*, 22(7), pp. 580-584.
6. Naqvi, W.M., Sahu, A. (2020). *Paradigmatic shift in the education system in a time of COVID 19 Evolution*. In *Journal of Medical and Dental Sciences*, 9 (27): 1974-1976, DOI: 10.14260/jemds/2020/430.
7. Pup, A. (15 March 2022). *Digitalizarea educației în ultimii doi ani de pandemie. Măsurile pe care autoritățile le-au promis și nu le-au realizat*.In *Libertatea*, https://www.libertatea.ro/stiri/digitalizarea-educatiei-in-ultimii-doi-ani-de-pandemie-masurile-pe-care-autoritatile-le-au-promis-si-nu-le-au-indeplinit-4031891, retrieved on 24 November 2022.
8. Schaefer, D., Coopersmith, J. (2018). *Kranzberg's Fifth and Fourth Laws*. In *Technology's Stories*, vol. 6, no. 4. DOI: 10.15763/jou.ts.2018.12.20.02
9. Tîrziu, A.M. (2015). *Protection and security of information at the level of national public authorities from Romania*. MPRA Paper 77711. München: University Library of Munich.
10. European Central Bank. (2022). *Digitalization and ECB strategy assessment. BCE*, https://www.ecb.europa.eu/home/search/review/html/digitalisation.ro.html, retrieved on 24 November 2022.

11. Centrul Național de Răspuns la Incidente de Securitate Cibernetică (CNRISC). (2019). *Evoluția amenințărilor în spațiul cibernetic românesc în anul 2018*. Directoratul Național de Securitate Cibernetică, https://dnsc.ro/vezi/document/raport-alerte-2018, retrieved on 26 August 2022.
12. European Commission. (2020). *New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient*, https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391, retrieved on 26 August. 2022.
13. *Digitalizarea sistemului educațional – propunere de politici publice* (4 June 2019), *Syene*, https://syene.ro/2019/06/04/digitalizarea-sistemului-educational-propunere-de-politici-publice/, retrieved on 24 November 2022.
14. ENISA (2015). *Definition of Cybersecurity – Gaps and overlaps in standardisation*, https://www.enisa.europa.eu/publications/definition-of-cybersecurity, retrieved on 24 November 2022.
15. ENISA. (2022). *Romania's National Cyber Security Strategy*. Work in progress, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/roncss.pdf, retrieved on 24 November 2022.
16. Ministry of Education and Research. (2020). Digitalization of education in Romania 2021-2027. *Modern and accessible school based on digital resources* – SmartEdu, online, https://www.smart.edu.ro, retrieved on 24 November 2022.