András Bencsik*
Mirosław Karpiuk**
Nicola Strizzolo***

Cybersecurity of E-government[1]

Abstract

Modern administration often uses ICT systems to deliver public services, which must be adequately secured. Public administration bodies must, therefore, also include cybersecurity in their policies. E-services should be the standard. Unfortunately, this standard does not always apply in administration. New technologies in a digital state and information society must be widely used, including by public bodies, so that the quality and accessibility of the services provided meet social needs. The public administration is responsible for continuously developing computerisation, making it possible to function normally in cyberspace where citizens have long been present.

Key words: e-government, cyber threats, cybersecurity.

* Assoc. Prof. András Bencsik, PhD, Faculty of Law, Eötvös Lóránd University, e-mail: bencsik.andras@ajk.elte.hu, ORCID: 0000-0001-5772-9968.

** Prof. Mirosław Karpiuk, PhD, Chair of Administrative Law and Security Studies, Faculty of Law and Administration, University of Warmia and Mazury in Olsztyn, e-mail: miroslaw.karpiuk@uwm.edu.pl, ORCID: 0000-0001-7012-8999.

*** Prof. Nicola Strizzolo, PhD, Department of Human Sciences, University of Udine, e-mail: nstrizzolo@unite.it., ORCID: 0000-0001-6384-9210.

1 This article is based upon work from COST Action CA20123 – Intergovernmental Coordination from Local to European Governance (IGCOORD), supported by COST (European Cooperation in Science and Technology). Project no. TKP2021-NVA-29 has been implemented with the support provided by the Ministry of Culture and Innovation of Hungary from the National Research, Development and Innovation Fund, financed under the TKP2021-NVA funding scheme.

Introduction

Public administration is established to meet societal needs, whether at the local, regional or central level. To be met effectively, these needs must take into account the preferences of their addressees. Such preferences, among others, include creating opportunities to contact the office via the Internet. This also applies to dealing with matters via the Internet. There is no modern administration without ICT systems used for its activities and, therefore, without e-public services.

Electronic services in the information society open up significant opportunities to meet the needs of such a society, including by public administration. However, if an e-government is to deliver public services efficiently, it needs to keep up with technological developments and should, therefore, meet the technical standards envisaged for such services. Services in the digital sector need to keep pace with emerging changes, so the public administration should continuously monitor and analyse them and, if necessary, adapt its actions to these changes.

The development of e-public services is hampered by certain legal obstacles that affect the smooth functioning of e-government, especially in the competitive market for information society services. The administration is obliged to act on the basis and within the law, including in the electronic market, which requires considerable mobility, and must keep up with the dynamics of the needs of the participants in such a market and the freedom of making decisions that apply there. Such freedom is not available to the administration, which can only take action that will fall within, or be related to, the public sphere.

Solutions to protect against cyber threats should be adequate to such threats, which are not fixed but dynamic. The mechanisms and tools must guard against threats rather than just identify, remedy or prosecute perpetrators. To achieve this, it is necessary not only to incur adequate financial outlays for purchasing modern cyber solutions and devices but also to have qualified staff[2]. E-government should invest in solutions that are adequate to the risks to provide its services electronically and seamlessly. It is also important to have appropriately trained personnel to handle e-services, including in terms of cybersecurity.

2 A. Bencsik, M. Karpiuk, M. Kelemen, E. Włodyka, *Cybersecurity in the Visegrad Group Countries*, Maribor 2023, p. 2.

The status of e-government in the public sphere and its cybersecurity

The goal of modern public administration is to create institutions that are stable and predictable. They should also be flexible enough to adapt to many social challenges, open to dialogue with the public and able to propose new solutions and improve their services. Nowadays, the concept of modern administration is linked to its modernisation, which, in all developed countries, is a basic indicator of public action. Significant studies synthesising knowledge in the field in question have been a consequence of the quite widespread conviction that the process of reforming the public sector of modern states, called, among others, the transformation of administration or the modernisation of administration, was aimed at searching for new concepts of the legitimacy of public administration activities, which would be more open in their relations with citizens[3].

Attention is drawn to the fact that public administration must take into account the principle that any new digital investment should be guaranteed an adequate level of cybersecurity. It happens that digital technologies are introduced faster than citizens can understand their impact. Therefore, education in the field of cyber threats and cybersecurity is very important[4]. Professional staff who carry out cybersecurity tasks and have the adequate knowledge, skills or competencies guarantee the quality of activities protecting cyberspace, contributing to optimising its operation and thus minimising disruptions occurring in this area[5].

The changes associated with the development of new technologies, which are used in many areas of life, force society to improve its knowledge and digital skills. Ongoing updating of knowledge and acquiring new skills makes it possible to adapt to an ever-evolving reality in which cyberspace is widely used. Digital competencies provide access to a wide range of services, so it is imperative to broaden them[6]. Digital competencies are also indispensable for

3 J. Blicharz, L. Zacharko, *Kilka refleksji na temat rozumienia nowoczesnej administracji publicznej*, „Gubernaculum et Administratio" 2022, no. 1, p. 10.

4 K. Gawkowski, *Cyberbezpieczeństwo w inteligentnym mieście*, „Cybersecurity and Law" 2023, no. 2, p. 104.

5 A. Bencsik, M. Karpiuk, *Cybersecurity in Hungary and Poland. Military aspects*, ibidem, no. 1, p. 83.

6 A. Bencsik, M. Karpiuk, N. Strizzolo, *Information Society Services and their Sybersecurity*, ibidem 2024, no. 1, p. 259.

the e-services provided by public administration and must be possessed by both the service provider and the user.

The ICT systems used by e-government to perform the tasks imposed on it must be efficient. Ensuring this agility requires a lot of investment (including financial) and continuous monitoring of threats.

ICT systems must be duly protected. E-government must, therefore, rely on cybersecurity, which the Polish legislator defines as resilience of information systems against actions which compromise the confidentiality, integrity, availability and authenticity of processed data, or the related services provided by those information systems[7]. Cybersecurity can be defined as a combination of technologies, processes, and practices designed to protect networks,

7 Art. 2 (4) of the National Cybersecurity System Act of 5 July 2018 (consolidated text, Journal of Laws 2023, item 913, as amended). For more information about cybersecurity refer to: M. Czuryk, *Cybersecurity as a premise to introduce a state of exception*, „Cybersecurity and Law" 2021, no. 2; J. Kulesza, *Należyta staranność a cyberbezpieczeństwo wewnętrzne organizacji* [in:] *Zagrożenia wewnętrzne bezpieczeństwa zasobów informacyjnych w organizacji*, ed. P. Dziuba, Warszawa 2023; M. Karpiuk, *Tasks of the Minister of National Defense in the area of cybersecurity*, „Cybersecurity and Law" 2022, no. 1; U. Soler, *The World of New, Virtual Trends – Central Europe Societies Touched by Covid-19*, „European Journal of Transformation Studies" 2020, no. 8; A. Pieczywok, *The use of selected social concepts and educational programmes in counteracting cyberspace threats*, „Cybersecurity and Law" 2019, no. 2; K. Kaczmarek, *Dezinformacja jako czynnik ryzyka w sytuacjach kryzysowych*, „Roczniki Nauk Społecznych" 2023, no. 2; M. Czuryk, *Supporting the development of telecommunications services and networks through local and regional government bodies, and cybersecurity*, „Cybersecurity and Law" 2019, no. 2; M. Karpiuk, *The Organisation of the National System of Cybersecurity: Selected Issues*, „Studia Iuridica Lublinensia" 2021, no. 2; A. Pieczywok, *Cyberspace as a source of dehumanization of the human being*, „Cybersecurity and Law" 2023, no. 1; J. Kurek, *Operational Activities in the Field of Cybersecurity* [in:] *Cybersecurity in Poland. Legal Aspects*, eds. K. Chałubińska-Jentkiewicz, F. Radoniewicz, T. Zieliński, Cham 2022; M. Karpiuk, *The obligations of public entities within the national cybersecurity system*, „Cybersecurity and Law" 2020, no. 2; M. Czuryk, *Restrictions on the Exercising of Human and Civil Rights and Freedoms Due to Cybersecurity Issues*, „Studia Iuridica Lublinensia" 2022, no. 3; M. Karpiuk, *The Local Government's Position in the Polish Cybersecurity System*, „Lex Localis – Journal of Local Self-Government" 2021, no. 2; M. Czuryk, *Special rules of remuneration for individuals performing cybersecurity tasks*, „Cybersecurity and Law" 2022, no. 2; K. Chałubińska-Jentkiewicz, *Cyberodpowiedzialność*, Toruń 2019; M. Czuryk, *The Legal Status of Digital Service Providers in the National Cybersecurity System*, „Cybersecurity and Law" 2024, no. 1; M. Karpiuk, W. Pizło, K. Kaczmarek, *Cybersecurity Management – Current State and Directions of Change*, „International Journal of Legal Studies" 2023, no. 2; M. Czuryk, *Cybersecurity and Protection of Critical Infrastructure*, „Studia Iuridica Lublinensia" 2023, no. 5; M. Adamczyk, M. Karpiuk, U. Soler, *The use of new technologies in education – opportunities, risks and challenges in the times of intensive intercultural change*, „Edukacja Międzykulturowa" 2023, no. 4; O. Evsyukova, M. Karpiuk, M. Kelemen, *Cyberthreats in Ukraine, Poland and Slovakia*, „Cybersecurity and Law" 2024, no. 1.

devices, programs, and data from attacks, damage, or unauthorised access[8]. Its role is to ensure that communication and information are safeguarded from external threats, and that critical infrastructure is resilient to possible attacks[9].

At present, it is difficult to predict the direction of future cyber threats and to unambiguously define their scope. What should not change, however, is the assumption that knowledge of cyberspace and the changes taking place in it should increase. Understanding, learning and updating how to obtain information, as well as learning about IT tools and their capabilities in the context of cybersecurity, are therefore fundamental to understanding cybersecurity[10]. The landscape of cyber threats is dynamic, and so must be the defence against them[11].

Cybersecurity of e-government includes, among other things, proper protection of its resources. Such protection measures include safeguarding digital content, ICT systems and devices, and safely transmitting content through these systems. For such protection to be effective, it is necessary to increase awareness of users who may become the targets of potential cyberattacks[12].

The pace of information technology development to date suggests that cyber threats may affect an ever-larger proportion of the population as well as have an increasing impact on the functioning of states[13]. It should be emphasised that cybersecurity, as one of the areas of security, especially today, where the rapid transmission of information is the basis of every activity and where digitisation determines the development of the state and society, must be particularly protected, even – where necessary – against individual freedoms and rights if the exercise of these cannot be reconciled

8 R. Buch, D. Ganda, P. Kalola, N. Borad, *World of Cyber Security and Cybercrime*, „Recent Trends in Programming Languages" 2017, no. 2, p. 18.

9 L. Maglaras, M.A. Ferrag, A. Derhab, M. Mukherjee, H. Jakicke, S. Rallis, *Threats, Countermeasures and Attribution of Cyber Attacks on Critical Infrastructures*, „EAI Endorsed Transactions on Security and Safety" 2018, no. 10.

10 J. Kołowski, D. Wesołek, *Informacje oraz ich dostępność w cyberprzestrzeni. Narzędzia oraz sposoby pozyskiwania i analizy informacji* [in:] *Zagrożenia wewnętrzne bezpieczeństwa…*, p. 76.

11 A. Bencsik, M. Karpiuk, *The legal status of the cyberarmy in Hungary and Poland. An overview*, „Cybersecurity and Law" 2023, no. 2, p. 28.

12 P. Romaniuk, *Kształtowanie administracyjnoprawnych warunków służących do budowy cyberbezpieczeństwa w administracji publicznej*, ibidem, p. 92.

13 K. Kaczmarek, *Zapobieganie zagrożeniom cyfrowym na przykładzie Republiki Estońskiej i Republiki Finlandii*, ibidem 2019, no. 1, p. 155.

with the need to ensure the cybersecurity of the state[14]. At the same time, it should be borne in mind that limitations in exercising constitutional rights and freedoms may be imposed only by statute and only when necessary in a democratic state for the protection of its security or public order or to protect the natural environment, health or public morals, or the freedoms and rights of other persons. Such limitations must not violate the essence of freedoms and rights[15]. Cybersecurity as an element of state security will, therefore, be able to provide a rationale for introducing limitations on individual freedoms and rights.

Public administration provides e-services in cyberspace. Cyberspace is defined as a global network consisting of interconnected ICT systems made up of devices that enable the creation, processing and exchange of information automatically between devices or knowingly and intentionally between their users[16]. For the efficient operation of the state, it is not only necessary to perform tasks with the use of cyberspace but also to ensure cybersecurity. However, the protection of cyberspace must be continuous, not only during crises or conflicts (although expressly in these cases) but also when the state is carrying out its tasks uninterruptedly[17]. Nevertheless, the extent of this protection may vary depending on the cyber threats that are happening or are likely to occur.

Public administration has been taking measures to support the development of e-services for many years. These include but are not limited to making a wide range of e-services available; increasing the efficiency of public administration through the implementation of interoperable IT solutions; providing from registers the public sector information used to extend the range of services offered; mutual recognition of ICT solutions and tools[18].

Broadening the range of e-services makes sense only if it is done following real social needs and expectations. The computerisation of public

14 M. Karpiuk, *The Protection of State Security in Cyberspace as a Justifying Ground for Restricting Constitutional Freedoms and Rights*, „Przegląd Prawa Konstytucyjnego" 2022, no. 3, p. 406.

15 Art. 3 of the Constitution of the Republic of Poland of 2 April 1997 (Journal of Laws 1997, no. 78, item 483 as amended).

16 K. Chałubińska-Jentkiewicz, M. Karpiuk, J. Kostrubiec, *The legal status of public entities in the field of cybersecurity in Poland*, Maribor 2021, p. 33.

17 A. Bencsik, M. Karpiuk, *Cybersecurity in Hungary and Poland*..., p. 83.

18 P. Romaniuk, *Szanse i zagrożenia dla administracji publicznej w świadczeniu usług drogą elektroniczną*, „Studia Prawnoustrojowe" 2022, no. 58, p. 442.

administration requires coherent strategies or policies that are an important factor in the rational use of funds from the state budget and the budget of the European Union. An important feature of e-government is the learning process for public administration employees and citizens alike. It should be emphasised that the mission of the public sector should be focused strongly on social needs and expectations[19].

In the case of e-government cybersecurity, it is also worth paying attention to planning. In its planning documents, the public administration sometimes has to take into account cybersecurity as an important element to ensure the efficient performance of public tasks through ICT systems that need to be protected against cyber threats. Planning, including planning for cyberspace, makes it possible to take coordinated action for the proper, timely and harmonious implementation of the objectives set for public administration in an organised and continuous manner[20].

Increasing the resilience of public administration information systems and achieving the ability to effectively prevent and respond to incidents is a critical objective of state policy. To ensure a secure and cost-optimal infrastructure for processing public administration IT systems, which is expected to benefit shortly from new forms of information processing and storage, among others, through the use of cloud computing services, it is postulated to prepare recommendations and promote good practices to increase resilience to potential cyber threats[21].

The results of digitisation in public administration in Hungary

Digitisation appears as an inevitable development path for public administration policymakers on the one hand, and, on the other hand, it can be understood as a broader category than the application of artificial intelligence,

19 Idem, *Rozwój elektronicznej administracji czynnikiem wspierającym nurt zarządzania humanistycznego*, „Journal of Modern Science" 2017, no. 33, p. 321.

20 M. Karpiuk, *Cybersecurity as an element in the planning activities of public administration*, „Cybersecurity and Law" 2021, no. 1, p. 46.

21 *Cybersecurity Strategy of the Republic of Poland for 2019–2024*, constituting an annex to Resolution No. 125 of the Council of Ministers of 22 October 2019 on the Cybersecurity Strategy of the Republic of Poland for 2019–2024 (Official Gazettel of Polish Government 2019, item 1037).

as the digitisation of public administration (operations) has a longer history and richer achievements. A brief overview and evaluation of developments in this field is presented below.

Géza Kilényi, a Hungarian scholar dealing with public administration law, once wrote in one of his studies that the history of public administration can be identified with the history of failed reforms, which, although an exaggeration, can be seen as an important reality. So the question arises: why has public administration consistently resisted the reform process, and why has there been so far no breakthrough in the context of digitalisation?

The first reason is the „historical specificity that after the regime change, large state institutes and state-owned companies with internationally significant R&D activities in science and technology have practically disappeared or have been privatised. Researchers were employed and generally engaged in selling products of foreign companies, so developing expert systems, a component of artificial intelligence, virtually stopped. At the same time, it seems appropriate to point out two historical facts for the sake of authenticity. On the one hand, it should be stressed that the priority in the development of public administrations after 1990 was to meet the requirements of the rule of law and democracy rather than to put them on a digital footing; on the other hand, in those sectors where IT developments did take place (more so in the mid-to-late 1990s), the isolated operation and sector-specific nature of the development of generic platforms was typical"[22].

On the other hand, it should also be stressed that the lack of credible „champions" was (and in some respects still is) one of the reasons for the digital explosion. In the work cited above, Erzsébet Fejes and Iván Futó refer to the phenomenon whereby the first initiative to implement a knowledge-based application usually comes from a vendor. „If the bidder is a large multinational company, it has several references in the field. The real question, however, is who needs to be convinced of the usefulness of the future application. The potential vendor needs to find an in-house »champion« who understands – perhaps already knows – the essential operational elements of the proposed solution, who is a sufficiently credible person and who is willing to stand behind

22 This trend has primarily affected the financial sector and more specifically the tax administration. For more on attempts to transform tax legislation, see Z. Ercsey, *Felelősség az adójogban*, „Glossa Iuridica" 2017, no. 2, p. 47–67.

the project, even »campaign« for it"[23]. Although the quotation suggests that this approach is more suited to the logic of the competitive sector, it has not, by definition, achieved breakthroughs in the public sector (and, given the nature of public procurement, can be a breeding ground for corruption), and so, there has long been understandable resistance to technological innovation and its management within public administrations and their staff. In the context of attempts at digitisation in public administration, I will look at the (instructive) institutionalisation of two legal instruments: electronic administration and the introduction of an electronic civil registry system.

The electronic civil status system was institutionalised by Act I of 2010 on the civil status procedure, which, according to the original plans, was to enter into force at the beginning of January 2011. What followed is known to all: the legislator „postponed" the entry into force first by one, then by two, and finally by three and a half calendar years, so the legislation eventually became applicable on 1 July 2014. For the purposes of this work, I will not go into the initial difficulties encountered in the early days. However, the circumstances that led to the delayed entry into force are certainly worth mentioning. There were two main reasons for the delay in entry into force. The first was the institutionalisation of registered partnerships, where there was no consensus between the concept of the law's proposer and that of the government in power at the time of its entry into force. This (political) conflict also hindered the final text of the law[24]. Simplifying what happened, there were, first of all, constitutional concerns about the introduction of registered partnerships, which were technical on the surface and political underneath. The professional argument was based on the desirability and constitutionality of institutionalising registered partnerships as a quasi-alternative to marriage (the first Constitutional Court decisions also addressed this question), but, in reality, it was the liberal/conservative approach to conservative family law legislation that decided the fate of the issue for a few years. This is related to our topic from the point of view that the new law introduced (in addition to the birth, marriage and death registers) the so-called fourth civil register, which did not help it to come into force at the initial date.

23 Cf. E. Fejes, I. Futó, *Mesterséges intelligencia a közigazgatásban – az érdemi ügyintézés támogatása*, „Pénzügyi Szemle" 2021, no. 1, p. 44.

24 The story began earlier: the first time the legal institution was dealt with was in AB 154/2008 (17.12.2008), but its satisfactory legal settlement was an obstacle to finalising the Civil Status Act.

The other reason for the „delay" is the lack of infrastructure: the electronic civil status system (and the security document register as part of it) was not built (forming a reliable system) by the deadline indicated, so the legislation was not ready to enter into force due to the lack of material conditions[25].

The introduction of electronic administration was not any smoother, but here the gap between the legislative plans and their actual realisation was even more pronounced. The first ambitious legislative attempt was Act CXL of 2004 on the General Rules of Administrative Procedure and Services (hereinafter: Ket.), which made provision for electronic administration under a separate title. Apart from the fact that the law (also) contained a lot of technical rules in this chapter, which led its critics to regard it as a „manual for administrators", it soon became apparent that the chapter introduced simply cannot work. To avoid giving a legal-historical aspect to this work, I shall illustrate the above by showing some of the original, difficult-to-enforce provisions of the Act: 1) „Unless otherwise provided by law, government decree or local government decree, the authority shall also conduct administrative matters by electronic means" [Ket. § 160(1)]; 2) „Where the public authority provides the possibility to use electronic administration or services not only through the central system, it shall also provide on its information platform information about the services available on the central system and the possibility to use them" [Ket. § 160(11)]; 3) „The authority may communicate by electronic mail only with a customer who has provided the authority with their electronic mail address for this purpose, for the validity of which the customer is responsible" [Ket. § 162(5)]; 4) „In the event of a temporary failure of the information technology system under the control of the public authority in the course of the ongoing electronic communication between the public authority and the customer, the public authority shall inform the customer of the fact of the failure by electronic mail, indicating the start and end time of the failure, within twenty-four hours after the failure has been rectified" [Ket. § 163(1) a].

In comparison, the first fine-tuning took place with the entry into force of the amendment to the Code of Laws (i.e. Act CXI of 2008): at that time, the legislator recognised that the previously declared state of digitisation of

25 It is worth noting that, in addition to the delay, this has further preserved an unconstitutional situation in which the subject matter was still regulated by decree-law and by decree of the Minister of the Interior until 2014, even though it was an exclusive legislative subject matter, which the Constitutional Court had already drawn the attention of the legislator to in 1990 in its decision no. 32/1990 (XII.22.) AB.

administration was more of an objective than a reality, so the procedural code only spoke of electronic information and electronic communication, and the technical provisions were transferred to Act LX of 2009 on electronic public services.

The final refinement was the amendment that only included in its principles the right of the customer to freely choose the means of communication with the public authority, with the electronic channel for communication being mandatory only between public authorities. This is essentially the model of today's legislation, according to which the provisions at the level of principles are laid down in Act CL of 2016 on the General Administrative Procedure, while the technical and other detailed rules are laid down in Act CCXXII of 2015 on the General Rules for Electronic Administration and Trust Services (Eüsztv.).

Both electronic administration, introduced as a general category, and the electronic civil status system raise the problem of the long-term storage of large amounts of data, many of which are sensitive. This poses a challenge for public administrations in two respects: on the one hand, the need to create a secure infrastructure with an increasing capacity to store the data in question in the long term, and on the other hand, the increased vulnerability of this data to cyber-attacks, as demonstrated by the attacks in cyberspace in recent years against several critical infrastructures (e.g. health data). Recognising this, the following section identifies the most pressing issues concerning long-term data storage.

For the authentication of electronically stored documents, electronic signatures are used. They use the private and public key pair of the Public Key Infrastructure framework. As part of this system, Certificate Authorities (CAs) issue certificates to their clients, which are nothing more than electronically signed certificates with an expiry date, in which the CA certifies to which client the public key belongs[26]. Given that the signature on this certificate is made with the CA's private key, which is authenticated by another CA, a certificate chain can be reached.

If there is no time stamp associated with the electronic signature, it is valid only as long as the certificate associated with the signature is valid. If the current one-year validity period is taken as a basis, this point cannot fulfil the condition of long-term validity. If the signature is accompanied by a time stamp and the signature was valid at the time the stamp was made, the signature should be

26 For more details on this point, see G. Gyurák, *Hosszú távú adattárolási szokások a digitálisan aláírt dokumentumok szemszögéből* [in:] *A hosszú távú adattárolás kérdései*, ed. I. Péter, Pécs 2014, p. 63–76.

considered valid beyond the expiry date of the certificates. This is very difficult to verify because, under current practice, the validity (OCSP) and revocation (CRL) lists mentioned above contain up-to-date data, and according to Art. 9(7) of Act XXXV of 2001 on Electronic Signatures (hereinafter „Eat."), data must be stored for ten years after the expiry of the signature certificate. The above should be checked for all elements of the certificate chain in addition to the signatory's certificate, and it may be difficult to collect this data, given that the certificates of a given certification service provider organisation may expire in the meantime and the organisation itself may cease to exist. In addition, the cryptographic procedures and encryption algorithms behind the above will become decryptable as technology develops, i.e. the cryptography used will no longer be secure. A solution to these problems may be provided by the PDF Advanced Electronic Signatures-Long Term Validity (PadES-LTV, Figure 1) developed by ETSI, which associates new validity data with a new timestamp within the validity period of the certificates associated with a given document and iteratively repeats this to maintain the validity of the document. This eliminates the need for cumbersome verification of certificate chain elements that may have been revoked, and the technology itself can ensure that state-of-the-art technologies are continuously applied, guaranteeing adequate security cryptography[27]. It is noted that using this technology can be advantageous even in the short term due to the one-year certificate validity period that is common in practice.

In the civil registry administration context, being the „flagship" of the state basic registers, it seems appropriate to refer to the principle of continuity. Continuity implies, on the one hand, that there should be no interruption in civil status registration activities and, more specifically, that there should be no period after the introduction of the state civil status registry during which no civil status events are registered in public. On the other hand, this specificity also means that civil status records must be retrievable at any time. This requirement (also) means that the state (or, more specifically, the legislator) must develop technical and IT solutions and systems that can stand the test of time and are capable of storing data of cardinal importance to the state in a secure and retrievable manner over the long term, both in terms of time and the volume of data to be registered.

27 For more information, see ETSI TS 102 778-4 V1.1.1 (2009-07) Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 4: PAdES Long Term - PAdES-LTV Profile.

Conclusion

Information systems are widely used by both private actors (including entrepreneurs) and by public bodies. Not only do they serve faster communication but are also used for performing tasks, including those of fundamental importance to the state and its institutions. They are important to the standard operation of the state and must, therefore, be protected to eliminate cyber attacks that disrupt their functioning[28]. Strategic tasks from the point of view of the operation of the state and its structures are also performed by public administration, using cyberspace to perform them. Due to the status of such tasks, the ICT systems through which they are performed must be particularly protected and secured against cyberattacks to ensure continued performance.

While the focus is often on technical solutions, the ethical dimension tends to be overlooked. However, security technologies have a profound impact on every individual's daily life. In this interconnected era, ensuring system security is crucial for the proper functioning of devices and networks, transcending mere data protection. Cyber-physical systems, like traffic lights or industrial control devices, have a direct impact on society, highlighting the importance of considering both technical and ethical challenges.

In summary, the scientific and technological community faces a multi-dimensional challenge: to protect digital infrastructure while acknowledging the profound interconnections between security and ethics. As technologies and societies progress, ethical guidelines must also evolve, ensuring a future where security and integrity coexist with innovation.

Bibliography

Adamczyk M., Karpiuk M., Soler U., *The use of new technologies in education – opportunities, risks and challenges in the times of intensive intercultural change*, „Edukacja Międzykulturowa" 2023, no. 4.

Bencsik A., Karpiuk M., *Cybersecurity in Hungary and Poland. Military aspects*, „Cybersecurity and Law" 2023, no. 1.

Bencsik A., Karpiuk M., *The legal status of the cyberarmy in Hungary and Poland. An overview*, „Cybersecurity and Law" 2023, no. 2.

Bencsik A., Karpiuk M., Kelemen M., Włodyka E., *Cybersecurity in the Visegrad Group Countries*, Maribor 2023.

28 M. Karpiuk, *Crisis management vs. cyber threats*, „Sicurezza, Terrorismo e Societa" 2022, no. 2, p. 121.

Blicharz J., Zacharko L., *Kilka refleksji na temat rozumienia nowoczesnej administracji publicznej*, „Gubernaculum et Administratio" 2022, no. 1.
Buch R., Ganda D., Kalola P., Borad N., *World of Cyber Security and Cybercrime*, „Recent Trends in Programming Languages" 2017, no. 2.
Chałubińska-Jentkiewicz K., *Cyberodpowiedzialność*, Toruń 2019.
Chałubińska-Jentkiewicz K., Karpiuk M., Kostrubiec J., *The legal status of public entities in the field of cybersecurity in Poland*, Maribor 2021.
Czuryk M., *Cybersecurity and Protection of Critical Infrastructure*, „Studia Iuridica Lublinensia" 2023, no. 5.
Czuryk M., *Cybersecurity as a premise to introduce a state of exception*, „Cybersecurity and Law" 2021, no. 2.
Czuryk M., *Restrictions on the Exercising of Human and Civil Rights and Freedoms Due to Cybersecurity Issues*, „Studia Iuridica Lublinensia" 2022, no. 3.
Czuryk M., *Special rules of remuneration for individuals performing cybersecurity tasks*, „Cybersecurity and Law" 2022, no. 2.
Czuryk M., *Supporting the development of telecommunications services and networks through local and regional government bodies, and cybersecurity*, „Cybersecurity and Law" 2019, no. 2.
Czuryk M., *The Legal Status of Digital Service Providers in the National Cybersecurity System*, „Cybersecurity and Law" 2024, no. 1.
Ercsey Z., *Felelösség az adójogban*, „Glossa Iuridica" 2017, no. 2.
Evsyukova O., Karpiuk M., Kelemen M., *Cyberthreats in Ukraine, Poland and Slovakia*, „Cybersecurity and Law" 2024, no. 1.
Fejes E., Futó I., *Mesterséges intelligencia a közigazgatásban – az érdemi ügyintézés támogatása*, „Pénzügyi Szemle" 2021, no. 1.
Gawkowski K., *Cyberbezpieczeństwo w inteligentnym mieście*, „Cybersecurity and Law" 2023, no. 2.
Gyurák G., *Hosszú távú adattárolási szokások a digitálisan aláírt dokumentumok szemszögéböl* [in:] *A hosszú távú adattárolás kérdései*, ed. I. Péter, Pécs 2014.
Kaczmarek K., *Dezinformacja jako czynnik ryzyka w sytuacjach kryzysowych*, „Roczniki Nauk Społecznych" 2023, no. 2.
Kaczmarek K., *Zapobieganie zagrożeniom cyfrowym na przykładzie Republiki Estońskiej i Republiki Finlandii*, „Cybersecurity and Law" 2019, no. 1.
Karpiuk M., *Crisis management vs. cyber threats*, „Sicurezza, Terrorismo e Societa" 2022, no. 2.
Karpiuk M., *Cybersecurity as an element in the planning activities of public administration*, „Cybersecurity and Law" 2021, no. 1.
Karpiuk M., *Tasks of the Minister of National Defense in the area of cybersecurity*, „Cybersecurity and Law" 2022, no. 1.
Karpiuk M., *The Local Government's Position in the Polish Cybersecurity System*, „Lex Localis – Journal of Local Self-Government" 2021, no. 2.
Karpiuk M., *The obligations of public entities within the national cybersecurity system*, „Cybersecurity and Law" 2020, no. 2.
Karpiuk M., *The Organisation of the National System of Cybersecurity: Selected Issues*, „Studia Iuridica Lublinensia" 2021, no. 2.
Karpiuk M., *The Protection of State Security in Cyberspace as a Justifying Ground for Restricting Constitutional Freedoms and Rights*, „Przegląd Prawa Konstytucyjnego" 2022, no. 3.
Karpiuk M., Pizło W., Kaczmarek K., *Cybersecurity Management – Current State and Directions of Change*, „International Journal of Legal Studies" 2023, no. 2.
Kołowski J., Wesołek D., *Informacje oraz ich dostępność w cyberprzestrzeni. Narzędzia oraz sposoby pozyskiwania i analizy informacji* [in:] *Zagrożenia wewnętrzne bezpieczeństwa zasobów informacyjnych w organizacji*, ed. P. Dziuba, Warszawa 2023.

Kulesza J., *Należyta staranność a cyberbezpieczeństwo wewnętrzne organizacji* [in:] *Zagrożenia wewnętrzne bezpieczeństwa zasobów informacyjnych w organizacji*, ed. P. Dziuba, Warszawa 2023.
Kurek J., *Operational Activities in the Field of Cybersecurity* [in:] *Cybersecurity in Poland. Legal Aspects*, eds. K. Chałubińska-Jentkiewicz, F. Radoniewicz, T. Zieliński, Cham 2022.
Maglaras L., Ferrag M.A., Derhab A., Mukherjee M., Jakicke H., Rallis S., *Threats, Countermeasures and Attribution of Cyber Attacks on Critical Infrastructures*, „EAI Endorsed Transactions on Security and Safety" 2018, no. 10.
Pieczywok A., *Cyberspace as a source of dehumanization of the human being*, „Cybersecurity and Law" 2023, no. 1.
Pieczywok A., *The use of selected social concepts and educational programmes in counteracting cyberspace threats*, „Cybersecurity and Law" 2019, no. 2.
Romaniuk P., *Kształtowanie administracyjnoprawnych warunków służących do budowy cyberbezpieczeństwa w administracji publicznej*, „Cybersecurity and Law" 2023, no. 2.
Romaniuk P., *Rozwój elektronicznej administracji czynnikiem wspierającym nurt zarządzania humanistycznego*, „Journal of Modern Science" 2017, no. 33.
Romaniuk P., *Szanse i zagrożenia dla administracji publicznej w świadczeniu usług drogą elektroniczną*, „Studia Prawnoustrojowe" 2022, no. 58.
Soler U., *The World of New, Virtual Trends – Central Europe Societies Touched by Covid-19*, „European Journal of Transformation Studies" 2020, no. 8.

Cyberbezpieczeństwo e-administracji

Streszczenie

Nowoczesna administracja do świadczenia usług publicznych często wykorzystuje systemy teleinformatyczne, które muszą być odpowiednio zabezpieczone. Dlatego organy administracji publicznej muszą w swojej polityce również uwzględniać cyberbezpieczeństwo. E-usługi powinny być standardem, ale, niestety, nie zawsze obowiązuje on w administracji. Nowe technologie w państwie cyfrowym i społeczeństwie informacyjnym muszą być powszechnie wykorzystywane, w tym przez podmioty publiczne, żeby jakość i dostępność świadczonych usług odpowiadała potrzebom społecznym. Na administracji publicznej ciąży obowiązek stałego rozwoju ukierunkowanego na informatyzację pozwalającą normalnie funkcjonować w cyberprzestrzeni, w której są już od dawna obecni obywatele.

Słowa kluczowe: e-administracja, cyberzagrożenia, cyberbezpieczeństwo