LEX LOCALIS

E-government in Visegrad Group Countries

Editors:
Gábor Hulkó
Mirosław Karpiuk
Jarosław Kostrubiec


§
LEX
LOCALIS

Title: E-government in Visegrad Group Countries

Editors: asst. prof., Gábor Hulkó, Ph.D. (Széchenyi István University of Győr, Faculty of Law and Political Sciences), prof. dr. habil., Mirosław Karpiuk, Ph.D. (University of Warmia and Mazury in Olsztyn, Faculty of Law and Administration), assoc. prof. dr. habil., Jarosław Kostrubiec, Ph.D. (Maria CurieSkłodowska University (Lublin), Faculty of Law and Administration)

Reviewers: assoc. prof. Pawel Romaniuk, Ph.D. (University of Warmia and Mazury in Olsztyn, Faculty of Law and Administration, Poland), assoc. prof. Andrius Puksas, Ph.D. (Vytautas Magnus University, Lithuania)

Kataložni zapis o publikaciji (CIP) pripravili v Narodni in univerzitetni knjižnici v Ljubljani

COBISS.SI-ID 267579139
ISBN 978-961-7124-29-3 (PDF)

First published in 2026 by
Institute for Local Self-Government Maribor
Medvedova ulica 12, 2000 Maribor, Slovenia
www.lex-localis.press, info@lex-localis.press

For Publisher:
prof. dr. Boštjan Brezovnik, director

Price:
free copy

https://doi.org/10.4335/2026.1 ISBN 978-961-7124-29-3 (PDF)

Available online at http://www.lex-localis.press.

E-government in Visegrad Group Countries

Editors:
Gábor Hulkó
Mirosław Karpiuk
Jarosław Kostrubiec

Maribor 2026

E-government in Visegrad Group Countries

GÁBOR HULKÓ, MIROSŁAW KARPIUK & JAROSŁAW KOSTRUBIEC

Abstract Modern countries need to pursue policies that are open to new technologies. This is not only due to widespread access to the Internet and but also to the necessity to build cyber-threat resilience. On the one hand, information technology allows public administrations to reach their addressees more quickly and more cost-effectively, while on the other hand, it poses new risks associated with the use of ICT systems that are not always correctly protected. These systems should operate smoothly or, if such disruptions occur, they should not disable the operation of public entities. Digital competences are also important, both regarding employees of public administration and the beneficiaries of the electronic services it provides. The monograph analyses the status of public administration in cyberspace. The legal basis for e-government in the Visegrad countries, where it is playing an increasingly important role in public life, has been discussed. Information society requires that the public administration meet its digital needs.

Keywords: • E-government • public administration • cybersecurity and cyber resilience • digital competences • information society • Visegrad Group countries

CORRESPONDENCE ADDRESS: Gábor Hulkó, Ph.D., Assistant Professor, Széchenyi István University of Győr, Faculty of Law and Political Sciences, 9026 Győr, Egyetem tér 1, Hungary, ORCID: 0000-0002-9139-6893, e-mail: hulko.gabor@ga.sze.hu. Mirosław Karpiuk, Ph.D., Prof. Dr. Habil., Full Professor, University of Warmia and Mazury in Olsztyn, Faculty of Law and Administration, Department of Administrative Law and Security Sciences, ul. Obitza 1, 10-725 Olsztyn, Poland, ORCID: 0000-0001-7012-8999, e-mail: miroslaw.karpiuk@uwm.edu.pl. Jarosław Kostrubiec, Ph.D., Dr. Habil. University Professor, Maria CurieSkłodowska University (Lublin), Faculty of Law and Administration, Plac Marii Curie-Skłodowskiej 5, 20-031 Lublin, Poland, ORCID: 0000-0003-1379-9846, e-mail: jaroslaw.kostrubiec@mail.umcs.pl.

https://doi.org/10.4335/2026.1 ISBN 978-961-7124-29-3 (PDF)
Available online at http://www.lex-localis.press.

Table of Contents

Introduction

The monograph is an outcome of the international research project "E-government in Visegrad Group Countries" aimed at identifying the place of e-administration in public space as well and its role in meeting social needs. The analysis covers the legal status of e-government in Poland, Hungary, Czech Republic and Slovakia. In view of the need to identify the place of e-government in the public domain, it was important not only to analyse the existing legal provisions governing its operation, but also to identify the problems it encounters in the practice of its work. The research assumptions required an analysis of both the adopted legal solutions and the organisation of e-government in each country forming the Visegrad Group. Discussing the solutions for the proper protection of IT aspects of its operation, including ensuring the protection of the ITC systems used by the e-government, including their cybersecurity, was an important direction of research, as reflected in the monograph.

Public administration is established to meet social needs at the local, regional and central levels. To be met effectively, these needs must take into account the preferences of their addressees, and such preferences also include the possibility of contacting the office via the Internet. There is no modern administration that would not use ICT systems for its activities, therefore there is no public administration without public e-services. Electronic services in the information society offer significant opportunities for meeting the needs of such a society, including by public administration. However, for e-government to be able to efficiently provide public services, it must use technological achievements and therefore meet the standards (including technical standards) required for this type of service (Bencsik, Karpiuk, Strizzolo, 2024: 147). In a digital state, public administration must meet the challenges posed by computerisation. Meeting the needs of society effectively means opening up to new technologies, which allows many matters to be handled remotely, thus without the need for eye-to-eye contact with public administration staff. Today, in the era of digital transformation, it is difficult to imagine any activity of the public administration without the use of ICT systems. Cyberspace is a place where not only citizens are active, but also where public entities provide services for the information society, which requires that administration is also digitally available.

Chapter I

Legal Bases for the Operation of E-government in the Czech Republic

ÁDÁM PÁL, HAJNALKA SZINEK CSÜTÖRTÖKI & GÁBOR HULKÓ

Abstract Effective public administration management is a dynamic process essential at both the Czech and international levels. In this context, e-government has emerged as a significant focus, representing a shift towards digital practices in public administration. Although e-government has become standard, continuous enhancements are crucial for improving effectiveness. Integrating digital technologies can enhance service delivery, transparency, and citizen engagement. Key areas for improvement include digital accessibility, strengthening telecommunications infrastructure, and the enhancement of e-proceedings and cybersecurity. This chapter analyzes the current state of e-government in the Czech Republic, assessing its legal framework and implementation. It highlights critical components such as electronic mailboxes, electronic submissions, and the delivery of official documents. Additionally, the chapter explores common areas of e-government, including administrative proceedings, tax administration, and communication with the Social Insurance Company and the courts, while examining the role of attorneys in utilizing electronic signatures and document conversion within the Czech legal system.

Keywords: • public administration • informatization • e-government • e-proceedings • the Czech Republic

CORRESPONDENCE ADDRESS: Ádám Pál, Ph.D., Senior Researcher, Central European Academy, 1122 Budapest, Városmajor utca 12-14, Hungary, ORCID: 0000-0002-6221-9572, e-mail: pal.adam@centraleuropeanacademy.hu. Hajnalka Szinek Csütörtöki, JUDr., dr. jur., LL.M., Ph.D. Candidate, University of Miskolc, Faculty of Law, Ferenc Deák Doctoral School of Law, 3515 Miskolc-Egyetemváros, Egyetem út 1, Hungary; Senior Researcher, Central European Academy, 1122 Budapest, Városmajor str. 12-14., Hungary, ORCID: 0000-0002-1535-6750, e-mail: hajnalka.szinek.csutortoki@centraleuropeanacademy.hu. Gábor Hulkó, Ph.D., Assistant Professor, Széchenyi István University of Győr, Faculty of Law and Political Sciences, 9026 Győr, Egyetem tér 1, Hungary, ORCID: 0000-0002-9139-6893, e-mail: hulko.gabor@ga.sze.hu.

https://doi.org/10.4335/2026.1.1 ISBN 978-961-7124-29-3 (PDF)
Available online at http://www.lex-localis.press.

1 Introduction

The 1990s marked a crucial era for the Czech Republic as it transitioned from a centrally planned economy to a market-oriented one, resulting in significant political, economic, social, and cultural transformations. Following necessary reforms, efforts began to modernize and digitalize public administration to enhance its efficiency and transparency (Brůna et al., 2005: 22). This period also triggered the development of information technology, prompting authorities to establish their internal information systems, which laid the groundwork for the introduction of e-Government in the country.

Moreover, national and international experts and organizations characterize the computerization efforts in the Czech Republic as a continuous endeavor, incurring billions of CZK annually (Veselý et al., 2016: 209; Bohatá et al., 2020: 1–2), underscoring the urgent need for a dependable method for authenticating and identifying citizens online (Dušek, 2023: 154).

In the context of rapidly advancing technology, modernizing public administration has become a top priority in the Czech Republic, as well as in other EU nations and globally. Information technologies have enabled the delivery of modern services, particularly in public sector governance. Over the past decade, there has been significant progress, from establishing initial e-government strategies to enacting relevant legislation, enhancing infrastructure, and developing electronic services, all while prioritizing cybersecurity. An effective e-government system can offer numerous benefits to the state, including cost savings, increased citizen engagement in public and political matters, and improved efficiency and transparency (Kolbenhayerová and Homa, 2022: 24).

This chapter aims to evaluate the current status of e-government in the Czech Republic by examining its fundamental legal framework and implementation. It emphasizes key aspects of e-government, including electronic mailboxes, electronic submissions from individuals and legal entities, and the delivery of official documents by public authorities. Furthermore, the chapter investigates frequently used areas of e-government, such as general administrative proceedings, tax administration, and interactions with the Social Insurance Company and the courts. It also considers the role of attorneys, particularly regarding electronic signatures, document conversion, and relevant elements of e-justice within the Czech Republic.

2 Legislative framework of e-government

The gradual development of e-government has naturally been reflected in its legal framework. A broad spectrum of legal regulations, including sub-legislative, statutory, and constitutional provisions is connected to the digitalization of public administration. However, due to the limitations of the present chapter and also the vast number of such

regulations, below we aim to briefly describe only the main regulations we consider important (for more information, see Kolbenhayerová and Homa, 2022).

First and foremost, the legal basis for e-government in the country is anchored in the Charter of Fundamental Rights and Freedoms (hereinafter referred to as the Charter), which is an integral part of the constitutional order. Specifically, Article 17(1) (division two – political rights) of the Charter guarantees the right to freedom of expression and the right to access information, which are fundamental principles for fostering transparency and participation in public affairs. This article not only protects the freedom of individuals to express their opinions but also ensures the right to seek, receive, and disseminate information without any restrictions. This provision is critical in laying the legal foundation for the development of e-government, as it ensures that citizens have the legal right to access public information and engage with public authorities openly and transparently. Moreover, as stated in Article 17(4), the freedom of expression and the right to seek and disseminate information may be limited by law where it is necessary in a democratic society for protecting the rights and freedoms of others, the security of the State, public security, public health, and morals.

Regarding the level of acts, the legislation concerning e-government can be divided into five main categories, which form the legislative and motivational framework for this area.

The first category includes laws that focus specifically on the digitalization process and e-government, covering areas such as the legal regulation of public administration information systems, core registries, and data integration. For example, Act No. 300/2008 Coll. on Electronic Acts and Authorized Conversion of Documents (hereinafter referred to as the Act on eGovernment),[1] Act No. 110/2019 Coll. on the Personal Data Processing, Act No. 250/2017 Coll on Electronic Identification, Act No 227/2000 Coll. on Electronic Signature, Act No. 499/2004 Coll. on Archiving and Records Management. The second category consists of legislation that addresses distinct aspects of e-government, including electronic documents, cybersecurity, and other related topics. For example, Act No. 181/2014 Coll. on Cybersecurity. The third category comprises procedural laws that govern general processes, such as the Administrative Procedure Code (Act No. 500/2004 Coll.), the Civil Procedure Code (Act No. 99/1963 Coll.)[2] , and the Tax Code (Act No. 280/2009).[3] The fourth category pertains to specific sectoral laws that dictate the procedures in particular areas, such as the Act No. 119/2002 Coll. Firearms Act, and the Road Traffic Act (Act No. 361/2000 Coll.). Lastly, the fifth category encompasses data entries maintained in the Register of Rights and Obligations, which serve as authoritative and binding records concerning the duties and operations of public administration. Act No. 499/2004 Coll. on Archiving and Records Management is a great example of that.[4]

According to Štědroň, the fundamental regulations of e-government also include Act No. 29/2000 Coll. on Postal Services, Act No. 101/2000 Coll. on the Protection of Personal Data, Act No. 106/1999 Coll. on Free Access to Information, and Act No. 480/2004 Coll.

on Certain Information Society Services (Štědroň, 2007). In his opinion, the legal framework governing e-government also encompasses various regulations that do not have the status of law. Alongside the primary laws, this foundational legislation also includes methodological instructions related to public administration information systems (ISVS) and implementing regulations, which are comprised of government and ministerial decrees. For example, Government Regulation No. 173/2006 Coll., which outlines the principles for determining fees and licensing payments for the provision of information under the Act on Free Access to Information, or Decree No. 194/2009 Coll., which specifies the details regarding the use and operation of the data box information system (Štědroň, 2007).

In 2017, the Czech government introduced the "Czech Republic 2030" strategy framework, a long-term plan focusing on sustainable development. Created through a participatory process involving the Office of the Government and the Council for Sustainable Development, this framework influences sector-specific strategies, including the Public Administration Reform (hereinafter referred to as the PAR) Strategy 2030. The PAR aligns public administration reform with the principles of "Good Governance" outlined in the Czech Republic 2030, promoting a resilient, flexible, and inclusive decision-making process (OECD, 2023). Key priorities include enhancing coordination between government bodies, boosting citizen engagement, and improving the efficiency, transparency, and accessibility of public services. The strategy also calls for the use of data-driven policy-making, digital transformation, and strengthening vertical coordination between central and local authorities.[5]

The modernization of the public administration has been a priority for the Czech government, reflected in its various strategies. The "Czech Point" project, for instance, has expanded digital services, but citizen satisfaction with administrative services remains low, emphasizing the need for further digitalization efforts. The "Digital Czech Republic Strategy" and the Czech Republic's EU Recovery and Resilience Plan further prioritize digital transformation and skill development (OECD, 2023).

Recent reforms include the creation of a Deputy Minister for Digitalization in 2021 and the upcoming Digital and Information Agency, which will centralize digital initiatives across ministries, underscoring the country's commitment to advancing digital governance (OECD, 2023).

Last but not least, the "Client-Oriented Public Administration 2030" concept serves as a strategic framework for the evolution of public administration in the Czech Republic for the decade spanning from 2021 to 2030 (Czudek, 2022). This initiative was established through Government Resolution No. 680 of 2014, which pertains to the Strategic Framework for Public Administration Development for 2014-2020, along with the formation of the Government Council for Public Administration (Government of the Czech Republic, 2014). Moreover, the National Information Strategy of the Czech

Republic focuses on six key goals, including user-friendly digital services for citizens and businesses, supportive digital legislation, ICT capacity building in public administration, central coordination of ICT, flexible digital offices, and comprehensive service accessibility across government platforms. This framework aims to modernize public services, streamline processes, and improve user accessibility and satisfaction by emphasizing unified digital channels, cross-departmental collaboration, and advanced technology integration (Government Resolution No. 736 of 2023).

3 Informatization of the public administration

The significance of digitization in today's world is undeniable. This concept, while somewhat abstract, is supported by specific insights from the Supreme Audit Office's summary report on the digitization of public administration in the Czech Republic (Kolbenhayerová and Homa, 2022: 25).

In recent years, the country has seen substantial investments in its information and communication technologies (ICT) infrastructure, resulting in significant technical advancements. This trend of investment is anticipated to continue. Between 2012 and 2018, state organizations and funds committed approximately CZK 75 billion to ICT, with around CZK 20 billion of that amount reimbursed through EU funds aimed at modernizing public administration. However, there are concerns that citizen engagement with digital services may not be as robust as expected (Kolbenhayerová and Homa, 2022: 25). According to a 2018 summary report, only 26% of individuals in the Czech Republic utilized online services to interact with government authorities. Additionally, statistics reveal that just 2% of private individuals have voluntarily registered for a data box, which is designed to simplify electronic communication with government agencies and, eventually, with individuals and organizations. A significant challenge for those who establish data boxes is their potential unawareness of the consequences of failing to access documents sent to them. Notably, in 2018, there were 97 million transactions conducted through data boxes, but only 0.65% of these were completed by non-business users (Supreme Audit Office, 2019).

Several factors contribute to the ineffectiveness of digital tools and the low adoption of digital public administration services. There is a lack of legislative readiness for further digitization, aging ICT systems within various sectors of public administration, poorly defined conditions for collaboration with external suppliers, a decentralized financial administration system, and insufficient staffing to maintain and modernize ICT systems. Among the various challenges identified, progress is being made in some areas. For instance, the Ministry of the Interior of the Czech Republic (hereinafter referred to as the MOI) has been designated as the primary coordinating body for information and communication technologies. The shortage of ICT personnel in public administration can be attributed to the very low unemployment rate in the Czech Republic, which was approximately 3.6% in the last quarter of 2021. While the number of employees in IT

services is on the rise, many are drawn to the private sector (Kolbenhayerová and Homa, 2022: 25).

Regarding the legislative framework for advancing the digitization of public administration in the Czech Republic, it remains a relatively recent development. The primary piece of relevant legislation is Act No. 12/2020. Coll., also known as the digital constitution, which governs individuals' and legal entities' rights to access digital services provided by public authorities. It outlines the rights to conduct electronic transactions in business and administrative contexts, mandates that public authorities offer digital services and accept electronic submissions, and specifies additional rights and responsibilities associated with these services (European Commission, 2018).

Finally, it is crucial to mention the country's National Recovery Plan, which aims to enhance digital public services through several integral components. These include Digital Services for Citizens and Businesses, Digital Systems of Public Administration, and Increasing the Efficiency of Public Administration Performance. The first component focuses on digitizing state and public administration functions, including healthcare, through a single, user-friendly interface accessed by a single login. Using federated portals like the Public Administration and Citizen Portals, this initiative aims to improve data management, electronic health services, and open data, saving up to CZK 25 billion annually and enhancing emergency resilience. The second component, the Digital Systems of Public Administration, supports the digitalization of public services, emphasizing data sharing, cybersecurity, and paperless processes. Key elements include developing registries, secure data handling, and establishing competency centers to support eGovernment, especially in healthcare. The third component seeks to improve public administration efficiency through evidence-based policy-making and client-centered services, including data sharing, central analytics, and training programs. With a total estimated cost of 76.7 million CZK, these efforts aim to make Czech public administration more efficient, coordinated, and digitally advanced.[6]

4 Digital accessibility of public administration

In July 2016, the United Nations Human Rights Council passed Resolution No. 38, which addresses the promotion, protection, and enjoyment of human rights on the Internet. Although this resolution is not legally binding, it has sparked discussions about the human right to access the internet and the freedom to use public virtual spaces. Similarly, the European Union has enacted numerous initiatives aimed at fostering the Digital Single Market in public services and administration to establish a modern and sustainable digital society that respects citizens' rights (Fiala and Sovova, 2020: 206.).

It is also important to highlight that in 2018, the Czech Republic enacted the Act on the Right to Digital Services[7] (Act No. 12/2020 Coll.), which fundamentally reshaped the landscape of public administration by recognizing the entitlement of citizens to access

digital services provided by public authorities. This law not only delineates the rights of individuals but also imposes clear obligations on public authorities to ensure the delivery of these digital services. It aims to facilitate a more streamlined interaction between citizens and the government, promoting the efficient provision of information and services through digital means. The act reflects a significant shift towards embracing technology in public governance, emphasizing that the availability of digital services is an essential aspect of modern citizenship in the digital age (Government of the Czech Republic, 2024: 11).

An essential legislative framework supporting the transformation of public administration is the Act on Public Administration Information Systems (Act No. 365/2000 Coll.). This act delineates the rights and responsibilities of all stakeholders involved in developing and managing public administration information systems, establishing a governance framework for their creation, usage, operation, and enhancement to meet the public's evolving needs. The Act also affirms citizens' rights to access electronic services from public administration, emphasizing that these services are voluntary. This digitization aims to enhance the rule of law and improve state functionality. Despite general familiarity with modern technologies among public officials and users, legal processes still often require personal confirmation or notarized signatures on paper documents. It seeks to unify fragmented legal frameworks and diverse administrative practices, as public servants currently lack a consistent approach to digital service delivery. While awareness of electronic communication opportunities is growing, many citizens still hold stereotypes that limit their engagement, resulting in the underutilization of digital services. Concerns arise regarding compulsory digitization potentially diminishing personal interactions in public administration and socially excluding vulnerable groups, such as the digitally illiterate or those without internet access. The fragmented legislative landscape fosters independent projects but complicates their application across the board (Government of the Czech Republic, 2024: 12).

One of the noteworthy amendments to this act occurred in September 2007, when the Czech Parliament sought to alleviate the administrative burden placed on citizens through the establishment of the Czech POINT network. This initiative enabled the general public to access transcripts and information statements from national registers with greater ease, thereby enhancing transparency and accessibility. Additionally, the 2007 amendment introduced a critical requirement mandating that all public authorities ensure their websites are accessible to individuals with disabilities. This incorporation of E-Accessibility into Czech legislation marked a significant step toward fostering an inclusive digital environment, recognizing the necessity of providing equal access to information and services for all citizens. The law further introduced new provisions addressing governance, economic efficiency, and security within public administration systems. The MOI assumed the long-term role of ICT governance coordinator, aligned with the overarching Information Conception of the Czech Republic approved by the government. This designation underscores the government's commitment to a

coordinated approach to information and communication technologies, reinforcing the infrastructure necessary for effective digital service delivery (European Commission, 2019: 14).

Moreover, the Act on Free Access to Information (Act No. 106/1999 Coll.) is fundamental in granting public access to information. In 2005, an amendment transposed EU Directive 2003/98/EC on re-using public sector information (PSI Directive). This amendment required public administrations to provide online information in open formats like XML to promote transparency and re-use of public data. Effective from January 2006, this amendment laid the foundation for a national open data catalog as a centralized platform for public data access, managed by the MOI, which has since published over 129,000 datasets. (European Commission, 2019: 14).

The MOI has issued guidelines to standardize data cataloging across central, regional, and local administrations. This initiative reflects the Czech government's commitment to transparency by facilitating public access to critical information.

In alignment with the Legislative Tasks Plan, the MOI drafted a further amendment to bring Czech law closer to European standards through Directive 2013/37/EU, which emphasizes open, machine-readable formats for public data. This draft was formally approved on 14 January 2015 via Decree No. 17 and enacted as Act No. 222/2015 Coll., effective from 10 September 2015. This amendment reinforced the national open data catalog as an information system and outlined public authorities' obligations to publish specific datasets (European Commission, 2019: 14).

By enshrining the right to digital services and ensuring open access to information, the government aims to empower citizens, promote transparency, and facilitate effective governance in an increasingly digital world. The ongoing efforts to refine and enhance these laws reflect a dedication to continuous improvement, ensuring that the public administration evolves in tandem with the technological advancements that characterize contemporary society. Through these initiatives, the Czech Republic is striving to create a more responsive and inclusive digital environment that meets the needs of all its citizens.

5 Electronic delivery

Since the early 1990s, the Czech Republic has been acquainted with the concept of eGovernment. However, it was only after 1999, when the internet began to emerge as a future-oriented technology, that it started to be adopted by public authorities and institutions of public administration. In 2003, the Ministry of Informatics was established, and three years later, the National Information and Communication Policy, known as e-Czech 2006, was introduced. During the same period, Czech POINT, a system of contact points for public services, was created, significantly advancing eGovernment in the

country, particularly in terms of services accessible to the public (Czech Statistical Office, 2018). As stated earlier, in 2008, the eGovernment Act was enacted, coming from the workroom of the MOI. It can be added that for proper fulfillment of its purpose, it requires the cooperation of various bodies, e.g., courts, the Ministry of Justice, or professional chambers – Czech Bar Association, Notarial Chamber of the Czech Republic, the Executor Chamber of the Czech Republic, etc. (Ščerba, 2009: 402). This act serves as the primary regulation for electronic delivery.

The scope of the act is outlined briefly in Section 1 of the legislation. Broadly, it covers three primary areas. The Act is designed to govern relations concerning electronic actions involving public authorities, municipal bodies, and other state institutions (such as Czech Television), including public notaries and court executors, in their dealings with both individuals and legal entities. Additionally, it applies to legal entities when interacting with state authorities. One of the key objectives of the Act is to facilitate more efficient, faster, and more advanced communication between state bodies, surpassing what is currently possible through conventional public administration channels. As stated in Section 1, the regulation of electronic communication between state authorities is a core aspect of the Act's application. The information system of data mailboxes constitutes the second significant level within the scope of the Act. This area of regulation is entirely new to the Czech legal framework, prompting Section 2 of the Act to offer a legal definition of the data mailbox, clarifying what this legal concept entails. According to this section, a data mailbox is defined as an electronic storage space designated for receiving communications from state bodies and for executing actions directed at those authorities. However, the Act fails to define the legal term "electronic data storage," which is crucial for understanding this context. This definition is notably absent from any currently applicable legal norms in the Czech Republic. Forthcoming bylaw legislation will likely need to provide a precise definition of this legal term to help eliminate interpretational issues and mitigate associated risks. If the elements defining "electronic data storage" remain unspecified, it could potentially lead to limitations or, in extreme cases, undermine the operations of entities utilizing electronic data storage in the relevant legal relationships. The third primary level in the scope of application of the Act pertains to the regulation of the authorized conversion of documents. Similar to the case with data mailboxes, the Act establishes a legal definition for this term in Section 22 (Ščerba, 2009: 405–406.).

In this regard, the aforementioned act also has several connections to Act No. 500/2004 Coll., Administrative Procedure Code. Act No. 300/2008 allows for electronic submissions to administrative authorities, which aligns with the provisions in the Administrative Procedure Code that specify how parties can communicate with administrative bodies. This legislation also anticipates the implementation of an electronic version of the official notice board. Authorities may establish their electronic notice boards indirectly by entering into public-law contracts with other agencies, particularly in cases where an administrative authority cannot publish content

electronically. However, the act does not specify the criteria for determining this lack of capability. Additionally, the Administrative Procedure Act includes similar obligations concerning electronic registries, which are designated offices within public authorities meant to facilitate the receipt and delivery of data messages as defined by the Act on Electronic Signatures (Špaček, 2012: 44).

The process for submitting documents to the administrative authority (to the MOI) during administrative proceedings is outlined generally in Sections 37(4) and (5) of the Administrative Procedure Code. Any submission, including supplementary documents related to an application, that is delivered in physical form (on paper) to the MOI, whether sent by mail or presented in person, must feature a received stamp from the MOI. This stamp must indicate the date of delivery for the correspondence.

When submissions are made by individuals or legal entities through their designated data box, there is typically no requirement for a guaranteed electronic signature. This is because the integrity of the document is inherently ensured by the data box system. Actions taken by an authorized individual through the data box carry the same legal validity as those made in writing and signed by that individual unless otherwise specified by legal regulations or internal rules requiring a collective action involving multiple individuals (for example, the signatures of both directors of a limited liability company, s. r. o.). In such cases, the electronic signatures of all involved parties must be attached to the data message, as detailed in Sections 8(1) to (4) and (6) and Section 18(2) of the Act on Electronic Actions and Authorized Document Conversion (MOI, 2024).

Conversely, if a submission is made electronically outside of the data box system—such as solely via email—it will only be deemed valid if it includes the guaranteed electronic signature of the submitter, as stipulated in Sections 37(4) and (5) of the Administrative Procedure Code.

When an authorized individual submits on behalf of another party via their own data box or email, a signed power of attorney must be included. If the power of attorney is in electronic form, it must either have the guaranteed electronic signature of the authorizer or be a product of authorized conversion. If it is a product of authorized conversion, it will display an attestation endorsement per Section 22 of the Act on Electronic Actions and Authorized Document Conversion.

Additional electronic documents submitted alongside the main application must also meet certain requirements. To have the same legal weight as notarized copies, these documents must be products of authorized conversion. Their status will be evident when opened, and they will carry the necessary attestation endorsement. Documents not undergoing authorized conversion, like simple scans, will be treated as ordinary, unattested copies lacking the same legal authority (MOI, 2024).

Authorized conversion refers to the process where a hard copy document, such as a power of attorney, is transformed into an electronic format by an authorized entity. This conversion includes verifying the document's content through an attestation endorsement. Authorized conversion entities are specified in Section 23 of the AEAAC, including designated offices like Czech POINT.

Finally, regarding the data boxes (Dušek, 2023: 8), it should be highlighted that if the document's characteristics permit it and a natural person, sole proprietor, or legal entity has an accessible data box, the MOI will send the document to that data box. However, this provision does not apply when delivery is made through public announcement or directly at the office. A document is considered delivered to a data box at the moment an authorized individual log into their account to access it. If that individual does not log in within 10 days following the document's delivery, the document will be regarded as delivered on the final day of this period. The delivery of a document to a data box carries the same legal weight as if it were handed directly to the recipient (MOI, 2024).

6 E-government and cybersecurity

The basis of cybersecurity regulation in the Czech Republic is established by Act No. 181/2014 Coll., on Cybersecurity[8] (commonly referred to as 'Cybersecurity Act'). This law, which came into effect at the beginning of 2015, serves as the cornerstone of the country's approach to protecting critical information infrastructure and securing cyberspace. As notable from its date of entry into effect, the Cybersecurity Act was implemented prior to the adoption of Directive 2016/1148 of the European Parliament and of the Council of July 6, 2016 (commonly referred to as 'NIS Directive'), the foundational piece of EU legislation aimed at achieving a high level of network and information systems security across the European Union.[9] In 2017, the Cybersecurity Act was amended to incorporate the NIS Directive's requirements. This revision also addressed practical challenges raised by the professional community, improving the law's overall effectiveness in safeguarding both public and private sectors (Studýnka, 2019: 23).

In addition to the Cybersecurity Act, the country's cybersecurity framework is further supported by several sub-statutory acts, which establish additional important rules. One of the key acts is Decree No. 82/2018 Coll., on Security Measures, Cybersecurity Incidents, Reactive Measures, Requirements for Submissions in the Field of Cybersecurity, and Data Disposal[10] (commonly and hereinafter referred to as the 'Cybersecurity Decree'). This decree implements specific provisions of the Cybersecurity Act by clarifying the tasks and responsibilities of obligated entities and outlining practical steps to ensure compliance with cybersecurity standards. Another important regulation is Decree No. 317/2014 Coll., on Significant Information Systems and Their Defining Criteria.[11] This decree defines which information systems are considered 'significant'[12] by establishing criteria for their identification, and it is particularly important for public

administration. From the perspective of public administration, Act No. 365/2000 Coll., on Information Systems of Public Administration,[13] along with its implementing regulations, also contains provisions relevant to the security of public administration information systems (Bajgar, 2024: 16-17).

The Cybersecurity Act does not explicitly define the term 'cybersecurity.' However, based on the definitions of related terms and the overall purpose of the Act, Maisner and Vlachová (2015: 62) characterize cybersecurity as a comprehensive set of educational and legal measures that ensure the protection of cyberspace, as encompassed within the Cybersecurity Act. According to Sec. 2 (a) of this Act, cyberspace is defined as the digital environment that enables the creation, processing, and exchange of information, comprising information systems, services, and electronic communication networks.

Section 21a and the subsequent provisions of the Cybersecurity Act designate the National Office for Cybersecurity and Information Security (*Národní úřad pro kybernetickou a informační bezpečnost, commonly referred to as 'NÚKIB'*) as the central authority for cybersecurity in the Czech Republic. It establishes and enforces security measures for information and communication systems handling classified information. NÚKIB coordinates responses during cybersecurity emergencies and collaborates with various stakeholders in the cybersecurity domain. The authority is also responsible for international cooperation, negotiating agreements related to cybersecurity. Additionally, NÚKIB oversees the monitoring of cybersecurity threats and incidents and informs the public as necessary. It develops the national cybersecurity strategy and updates it at least every five years. Furthermore, NÚKIB certifies cybersecurity practices according to EU regulations and identifies operators of essential services, ensuring they comply with sector-specific cybersecurity criteria.

The Cybersecurity Act designates in Section 3 several categories of obliged entities, including operators of electronic communication services, administrators and operators of critical information infrastructure, significant information systems, and basic services, as well as digital service operators. Administrators are entities that determine the purpose and conditions for processing information or operating a communication system, while operators ensure the functionality of the technical and programmatic means that constitute these systems. Given the rapid pace of digitalization in government operations, which has already seen significant implementation in practice (see above), many public administration bodies also qualify as obliged entities under this Act. This evolution emphasizes the necessity for these bodies to adhere to cybersecurity regulations to protect critical information and services.

The most basic obligations of obliged entities include registration with the NÚKIB by providing their contact details as required under Section 16 of the Cybersecurity Act, and establishment and implementation of security measures under Section 4 to protect their systems from cyber threats. In the event of a cybersecurity incident, these entities are

required to report it to the relevant authorities as stipulated in Section 8. Furthermore, they must continuously carry out security measures as outlined in Section 11 to ensure ongoing protection against potential cyber risks.

Public authorities that administer or operate information systems often play a crucial role in maintaining the overall functionality of the state. Consequently, such systems have a higher significance accompanied by a heightened security exposure as well. The Cybersecurity Act considers this aspect and classifies these public bodies as operators or administrators of 'significant information systems,' which are defined as systems of 'higher general importance for the functioning of the state or with higher security exposure' (Polčák et al., 2018: 598). This designation underscores the necessity for enhanced protection measures, as well as elevated attention and resources to ensure their resilience against cyber threats.

Significant information systems (hereinafter also referred to as 'SIS') are defined in Section 2 (d) of the Cybersecurity Act as information systems managed by public authorities, which are neither critical information infrastructure[14] nor basic service information systems. A key characteristic of SIS is that they are managed by entities considered public authorities.[15] However, not all systems operated by public authorities qualify as SISs, only those, where a security breach could substantially impede or jeopardize the operations of the managing public authority.

The Cybersecurity Decree provides detailed criteria for identifying which information systems qualify as SIS, specifying in Section 2 that these systems are managed by public authorities and utilized for essential functions listed in the Decree. Section 3 of the Decree then establishes the exact conditions under which a security breach could significantly disrupt the operations of these authorities. Importantly, the Cybersecurity Decree also clarifies in Sec. 2 para. 3 that systems managed by local self-government (municipal) authorities are explicitly excluded from this designation, thereby ensuring that only those systems deemed vital to the functioning of higher-level public authorities are categorized as SIS.

In addition to the general obligations of all obliged entities under the Cybersecurity Act specified above, administrators and operators of significant information systems are required to fulfill several specific responsibilities. These include promptly notifying each other when a system meets the criteria to be classified as a SIS, implementing and documenting necessary security measures tailored to their systems, and ensuring that security requirements are considered when selecting contractors for the SIS. They must also establish specific security protocols for cloud computing services, detect cybersecurity events, and immediately report any incidents to the relevant authorities. Furthermore, they are obligated to take reactive measures as instructed by NÚKIB and to report the results of these actions. Additional responsibilities include safely managing data and operational information during the operation and termination of the SIS, as well

as complying with data requests from NÚKIB in the event of a cybersecurity threat (see Studýnka, 2019: 38-39).

7 Supporting the development of telecommunication services and networks

The Czech Republic is actively supporting the development of telecommunications services and networks through a strategic approach designed to ensure high-speed internet access for all households, institutions, and businesses across the country, aligning with the short-term objectives outlined in the EU regulatory framework for this sector. The core of this effort lies in the National Plan for the Development of Very High-Capacity Networks[16] (VHCN), which aligns with broader government strategies such as 'Digital Czech Republic' (*'Digitální Česko'*) and the Innovation Strategy of the Czech Republic 2019–2030. The focus is on creating a robust digital infrastructure to support the growing demand for high-speed internet services (Ministry of Industry and Trade, 2021: 5).

The legal basis for the development of telecommunications networks is rooted in both national and European legislation. Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code, which plays a significant role in the field was incorporated into Czech law through amendments to Act No. 127/2005 Coll. on Electronic Communications and Amendment to Certain Related Acts[17] (Electronic Communications Act). Additionally, Act No. 194/2017 Coll. on Measures to Reduce the Costs of Deploying High-Speed Electronic Communications Networks and Amendment to Certain Related Acts,[18] which – as its name indicates – focuses on reducing the costs of deploying high-speed networks, also supports the expansion of telecommunications infrastructure by ensuring more efficient processes and access to critical infrastructure.

Several key public bodies are responsible for implementing and overseeing the development of telecommunications networks in the Czech Republic. The Ministry of Industry and Trade (*Ministerstvo průmyslu a obchodu*) (hereinafter referred to as 'MPO') is at the forefront of this effort, bearing the primary responsibility for formulating and executing the national strategy for telecommunications. The MPO oversees the implementation of the National Plan for the Development of VHCN and manages public funding for the deployment of telecommunications infrastructure. It plays a central role in coordinating the use of EU structural funds and ensuring compliance with both national and EU regulations (Ministry of Industry and Trade, 2021: 39).

The Czech Telecommunication Office (*Český telekomunikační úřad*) (commonly known as 'ČTÚ') serves as the regulatory authority for the telecommunications market. Its responsibilities include monitoring the state of network development and conducting analyses to identify regions where high-speed internet access is lacking. ČTÚ's comprehensive data collection and mapping efforts are critical for determining where government intervention is needed, especially in so-called white areas—regions with

insufficient or no access to high-speed internet. ČTÚ also plays a role in regulating market competition and ensuring that private investments are not undermined by public interventions (Ministry of Industry and Trade, 2021: 39).

The Agency for Business and Innovation (*Agentura pro podnikání a inovace*) (known as 'API') is instrumental in managing subsidy programs for businesses involved in telecommunications infrastructure projects. Through the Operational Programme Enterprise and Innovation for Competitiveness (OP PIK), API provides financial support to companies that invest in expanding high-capacity networks, particularly in regions where private investment alone is not sufficient to achieve full coverage (Ministry of Industry and Trade, 2021: 40).

The Czech government's approach to telecommunications development primarily encourages private sector investment in expanding networks. In most areas, private companies are responsible for building and operating high-speed networks. However, the government intervenes in white areas where the market fails to deliver adequate infrastructure. These are typically rural or less economically viable regions where private companies have little incentive to invest due to high costs and low profitability. In such cases, the government provides subsidies to stimulate development (Ministry of Industry and Trade, 2021: 24-25, 28).

These subsidy schemes, largely funded by the European Structural and Investment Funds (ESIF), are designed to support network expansion in underserved regions. The Operational Programme Technology and Applications for Competitiveness (OP TAK) is the primary mechanism through which businesses can access these subsidies. The process begins with ČTÚ identifying white areas through its mapping and analysis efforts. Once these regions are identified, businesses can apply for financial support to develop telecommunications infrastructure in these areas. The decision-making process is competitive, with applications evaluated based on criteria such as efficiency and cost-effectiveness. The Ministry of Industry and Trade, in collaboration with ČTÚ and API, decides on and oversees the allocation of subsidies, ensuring that public funds are directed to regions where they will have the greatest impact (Ministry of Industry and Trade, 2021: 28-29).

The overall goal is to limit government intervention to areas where market mechanisms do not function effectively, allowing private companies to lead the development of telecommunications networks in more profitable regions. By complementing private sector engagement with regulatory oversight and public funding, the Czech Republic is working towards its vision of comprehensive digital connectivity, ensuring that even the most remote regions have access to high-speed internet services by the end of this decade.

8 Minister responsible for informatization and his responsibilities

Currently, the Czech Republic does not have a dedicated ministry exclusively focused on informatization or digitalization. However, this was not always the case. Between 2003 and 2007, the Czech government operated the Ministry of Informatics (*Ministerstvo informatiky České republiky*) established under Act No. 517/2002 Coll.,[19] which was the central administrative authority responsible for information and communication technologies, electronic communications, and postal services. It was responsible for coordinating the development of e-government, promoting fair competition in telecommunications, supporting e-commerce growth, and enhancing computer literacy in the country. However, the ministry was short-lived, operating for only four years before being dissolved in 2007 by Act No. 110/2007 Coll.[20] Upon its dissolution, its agenda was largely transferred to the Ministry of the Interior, while certain responsibilities were redistributed to the Ministry of Industry and Trade and the Ministry of Regional Development.

Despite its abolition, the need for a centralized body to manage informatization remained present in Czech political discourse, continuing to surface in the years that followed. Notably, in the 2021 election campaign, the Pirates and Mayors (*Piráti a Starostové*) coalition advocated for the creation of an institution that would unify and manage IT projects across the public administration (Piráti a Starostové, 2021). Their proposal envisioned a team tasked with providing methodological and practical support to governmental offices, coordinating IT projects, and advancing the full digitalization of public administration processes.

While the Pirates and Mayors coalition, which became part of the incumbent Czech government, did not succeed in creating a separate ministry for digitalization, a compromise was reached. The position of Deputy Prime Minister for Digitalization (*Místopředseda vlády pro digitalizaci*) was established, operating without a dedicated ministry but supported by a specialized cabinet within the Office of the Government of the Czech Republic (*Úřad vlády ČR*). This new role meant that the position of the Government Commissioner for Information Technology and Digitalization (*Vládní zmocněnec pro informační technologie a digitalizaci*), which had previously served as the primary coordinating body for digitalization efforts, became obsolete and was dissolved at the beginning of 2022 (ČTK, 2022).

The Deputy Prime Minister's role focuses on advancing key areas of digitalization in the Czech public sector. The overarching goals are to increase transparency, streamline services for citizens, and improve efficiency within public administration. A key principle of the digitalization agenda is that data, not citizens, should move between government offices, thus saving time for both citizens and civil servants. Among the initial goals upon establishing the Deputy Prime Minister for Digitalization position were the introduction of electronic personal identification documents and the complete digitalization of

building permit processes, deemed essential for enhancing efficiency. Additionally, the formation of central coordination teams was planned to ensure the cost-effectiveness and smooth implementation of the digitalization initiatives (Ministry of Regional Development of the Czech Republic, 2022).

An important step taken by the Deputy Prime Minister for Digitalization was the establishment of the Digital and Information Agency (*Digitální a informační agentura*), by Act No. 471/2022 Coll., which amended the above-mentioned Act No. 12/2020 Coll., on the Right to Digital Services and Amendments to Certain Acts. Under Section 2a. of the latter, the Digital and Information Agency serves as the central administrative authority for electronic identification, trust services, and public administration information systems. Its key tasks include coordinating digital services and transactions, overseeing information technology initiatives, managing data sharing practices, and ensuring the provision of central communication support for public administration. Additionally, the agency is responsible for professional development, training, and knowledge sharing in its areas of expertise, as well as operating competence centers to enhance digital capabilities across government entities.

In addition to establishing the Digital and Information Agency, the Deputy Prime Minister for Digitalization has initiated several important projects in recent years. These include the launch of eDocuments, benefiting over half a million citizens; enhancements to the Citizen Portal, which expanded services from 29 to over 600 and attracted more than 1.4 million users; and the introduction of the Digital Representation Register to streamline digital power of attorney processes. Preparations are also underway for the Digital Services Act, set to be fully implemented in February 2025 (Neščivera, 2024).

Despite the various initiatives undertaken by the Deputy Prime Minister for Digitalization, the effort to advance the digitalization of building permit processes faltered. The issue turned into a political controversy, casting a shadow over the office's overall effectiveness. As a result of delays with this task, the Prime Minister decided to recall the Deputy Prime Minister for Digitalization (Hroch & Stuchlíková, 2024). As of October 2024, the position remains unoccupied, further complicating efforts in this area and casting doubt on the future coordination of digitalization initiatives in the country.

9 Administrative e-procedure

The administrative procedure in the Czech Republic is governed by Act No. 500/2004 Coll., the Code of Administrative Procedure[21] (hereinafter referred to as 'CAP'), which primarily regulates administrative processes in general. However, the Act also addresses key provisions that enable the digitalization of these procedures, facilitating the use of electronic tools to improve the efficiency and accessibility of public services for citizens and businesses.

Section 37, paragraph 4 of the CAP allows for the submission of documents electronically. To comply with the specific requirements for such submissions, as outlined in Act No. 297/2016 Coll., on Trust Services for Electronic Transactions, only recognized electronic signatures are permitted. Specifically, under Section 6 of this Act, this means that when submitting an electronic document to a public authority or other relevant entities, it must be signed with a recognized electronic signature. This is defined as an advanced electronic signature based on a qualified certificate or a qualified electronic signature. In the sixth paragraph of Section 37, the CAP also anticipates situations where a public authority is unable to receive electronic submissions as required by Section 37, paragraph 4. In such cases, the authority must enter into a public-law agreement with a municipality with extended powers (*obec s rozšířenou působností*) based on the place of its seat, allowing this municipality to operate an electronic submission system on behalf of the authority and ensuring that electronic submissions can be processed despite the authority's limitations.

In addition to the above, electronic submissions can also be made through data boxes (*datové schránky*) as specified in Act No. 300/2008 Coll., on Electronic Acts and Authorized Conversion of Documents. According to § 18, paragraph 2 of this Act, any submission made by a person through a data mailbox has the same legal effect as a written and signed submission, unless otherwise stated by a specific act. While the Code of Administrative Procedure does not explicitly mention the use of data mailboxes, this method is also fully recognized as a valid way to submit documents electronically (Ministry of the Interior, 2018).

If a submission is made electronically but not in a qualified form, the applicant must supplement the submission by adding the necessary signature or submitting a written or oral confirmation within five days. Failure to comply with this requirement renders the submission legally ineffective, as affirmed by the Supreme Administrative Court in decision 9 As 90/2008-70. Furthermore, according to the same ruling, the legal framework does not obligate public authorities to inform applicants about the necessity of supplementing or confirming submissions made without the required qualified form within the stipulated timeframe (Supreme Administrative Court, 2009). This means that public authorities are not legally required to provide guidance to applicants regarding the completion of their submissions, even though they are encouraged to do so under the principle of good administration. This lack of obligation may lead to certain complications in the processing of electronically filed documents (Ministry of the Interior, 2018).

Public authorities in the Czech Republic, like other participants in administrative proceedings, have the capacity to conduct their actions electronically. According to Section 19, paragraph 1 of the CAP, documents must primarily be delivered by the public authority that generated them through the public data network to the recipient's data box.

Only if electronic delivery is not possible can the authority deliver the document directly or by other means.

According to Section 19, paragraph 4 of the CAP, public authorities are permitted to deliver documents to a simple electronic address specified by the applicant, provided that it is not prohibited by law or the nature of the matter, especially when this can expedite the process. When making decisions or issuing documents electronically, the public authority is responsible for preparing the electronic version of the decision, as outlined in Section 69, paragraph 3 of the CAP. In performing these actions, public authorities utilize a qualified electronic seal. According to the previously mentioned Act No. 297/2016 Coll., when not stated otherwise, public authorities may seal the document with a qualified electronic seal under Section 8 of this Act. This seal is recognized as valid for acts performed in the exercise of their authority and ensures the authenticity of electronic documents.

The right to access administrative files in the Czech Republic is outlined in Section 38 of the CAP. This right includes the ability to make excerpts, obtain copies, or request that the administrative body provide copies. However, the CAP does not explicitly state that this right can be exercised remotely in a digitalized form. This issue is addressed in a report published by the Czech Ombudsman, which reveals that the practice of remote access to administrative files remains inconsistent across public authorities. Some bodies permit remote file access, sending documents via data boxes or email, while others cite technical or logistical challenges, particularly when converting documents from paper to electronic form or verifying their authenticity (Office of the Public Defender of Rights, 2018).

Furthermore, there is variability regarding administrative fees for providing copies; some authorities charge fees, especially when authentication is involved, while others do not. This inconsistency creates unequal treatment of applicants and highlights the need for clearer legislative or methodological guidelines to standardize the application of this right across public administration, including its remote implementation.

While many aspects of the electronic administrative procedure in the Czech Republic are well-regulated and supported by legislation, there remain areas that could benefit from further refinement. Inconsistencies in practices, such as the variability in remote access to administrative files and the lack of unified approaches to associated administrative fees, reveal areas where improvements are needed. To make the system more streamlined and consistent, clearer legislative or methodological guidelines could address the remaining gaps, particularly as it is increasingly evident that electronic access to administrative procedures will become even more common in the years to come.

10 Conclusions

The Czech Republic has made substantial progress in e-government by investing in digital transformation across various public sectors. Legislative frameworks, starting from the fundamental principles of the Charter of Fundamental Rights and Freedoms, underscore the commitment to transparency, citizen participation, and accessible public information. Core regulations in the field such as the Act on e-Government, the Cybersecurity Act, and the Act on the Right to Digital Services have established a solid foundation for implementing e-government initiatives, covering electronic identification, data protection, and cybersecurity.

Despite these advancements, certain areas present ongoing challenges, particularly in ensuring consistent digital accessibility and citizen engagement. While investments in ICT infrastructure and projects like Czech POINT have improved accessibility, adoption remains low among citizens, partly due to limited awareness and engagement. The government's initiatives to support digital public administration, including the introduction of data boxes and the anticipated Digital Services Act, aim to simplify interactions with government institutions, but further education and support may enhance citizen uptake.

Moreover, cybersecurity remains a priority, with NÚKIB coordinating responses to digital threats across critical public administration systems. As digitalization deepens, these systems become increasingly essential to state functionality, requiring robust security and regulatory oversight to protect sensitive data and maintain public trust. The upcoming transposition of the NIS2 Directive into the Czech legal framework will strengthen this oversight by introducing stricter security requirements and expanding the range of entities subject to cybersecurity regulations.

Moving forward, the Czech Republic's strategic plans, including the National Recovery Plan and the Czech Republic 2030 framework, set ambitious targets for a fully digital and interconnected society. However, achieving these goals will require not only ongoing improvements in ICT coordination, more extensive citizen education, and refined legislative support but also a recognition of the complexities involved. The challenges are not easy to overcome, as demonstrated by the setbacks in the digitalization of building permit processes. This experience underscores the importance of careful planning and steady commitment to make digital services accessible and efficient for all citizens.

Notes:

[1] The Act came into effect on 1 July 2009 to ensure the best possible conditions for communication between citizens and authorities in electronic form. See Uhlířová, 2012.
[2] In the case of electronic legal actions, the general provisions outlined in Section 561(1) of Act No. 89/2012 Coll., the Civil Code apply. This provision states that for a legal act made in written form to be valid, a signature of the acting party is required, which may be replaced by mechanical means, where customary. The third sentence of this provision specifies that the conditions for electronic signing of documents in legal acts performed through electronic means are set by other legal regulations. One such regulation is the eIDAS regulation, and another is Act No. 297/2016 Coll., on Trust Services for Electronic Transactions. Section 562(1) of the Civil Code further stipulates that the written form is preserved even in legal acts carried out through electronic or other technical means that allow the content and the identity of the acting party to be recorded. See Švadlena and Švecová: 2023.
[3] Concerning the field of digitalization of tax administration.
[4] See the website of the National Architecture of eGovernment: https://archi.gov.cz/znalostni_baze:klicove_zakony_eg (Accessed: 14 October 2024)
[5] Find out more about the strategy: https://vlada.gov.cz/assets/ppov/udrzitelny-rozvoj/projekt-OPZ/Strategic_Framework_CZ2030.pdf (Accessed: 14 October 2024)
[6] For more information see the website of the Ministry of Interior: https://www.mvcr.cz/npo/komponenty.aspx. (Accessed: 25 October 2024)
[7] Zákon č. 12/2020 Sb. o právu na digitální služby a o změně některých zákonů.
[8] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).
[9] Since the adoption of the NIS Directive, the EU cybersecurity framework has been updated by Directive (EU) 2022/2555 of the European Parliament and of the Council (referred to as the NIS2 Directive), which repealed the original NIS Directive. The NIS2 Directive introduces stricter security requirements and extends the scope of entities subject to cybersecurity regulations. However, as of early October 2024, this updated directive has not yet been transposed into the Czech legal framework. The transposition of the NIS2 Directive into the Czech cybersecurity system will not only broaden the scope of obliged entities but also introduce additional responsibilities for public authorities that are considered obliged entities (see Bajgar, 2024).
[10] Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti).
[11] Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích.
[12] 'Significant information systems' represent a specific legal category of information systems that are subject to distinct obligations regarding cybersecurity (see below).
[13] Zákon č. 365/2000 Sb., Zákon o informačních systémech veřejné správy a o změně některých dalších zákonů.
[14] The reason for excluding this category is that it represents an even more specific type of information system that is provided with additional protection measures according to the Cybersecurity Act.
[15] According to a widely cited definition by the Constitutional Court of the Czech Republic (1993), 'public authority refers to any authority that makes authoritative decisions regarding the rights and obligations of individuals, either directly or indirectly. In this context, the subjects affected by these decisions are not on equal footing with the public authority, and the outcomes of such decisions do not depend on the will of the affected parties.'

[16] Ministry of Industry and Trade [Ministerstvo průmyslu a obchodu]. (2021). National Plan for the Development of Very High-Capacity Networks [Národní plán rozvoje sítí s velmi vysokou kapacitou]. Retrieved from https://www.mpo.gov.cz/assets/cz/e-komunikace-a-posta/elektronicke-komunikace/koncepce-a-strategie/narodni-plan-rozvoje-siti-nga/2021/3/149908-21_III_mat_VHCN.pdf

[17] Zákon č. 127/2005 Sb. o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích).

[18] Zákon č. 194/2017 Sb. o opatřeních ke snížení nákladů na zavádění vysokorychlostních sítí elektronických komunikací a o změně některých souvisejících zákonů.

[19] Zákon č. 517/2002 Sb., kterým se provádějí některá opatření v soustavě ústředních orgánů státní správy a mění některé zákony.

[20] Zákon č. 110/2007 Sb., o některých opatřeních v soustavě ústředních orgánů státní správy, souvisejících se zrušením Ministerstva informatiky a o změně některých zákonů.

[21] Zákon č. 500/2004 Sb., Správní řád.

Chapter II

Legal Bases for the Operation of E-government in Hungary

BERTOLD BARANYI, ANDRÁS BENCSIK & ISTVÁN HOFFMAN

Abstract It should be emphasised that the Hungarian regulation on electronic administration has started to develop during the Millennia, and the former restrictions of the electronic administration have been eliminated, and even the practice of the Hungarian e-administration has been transformed by the ICT revolution and the new legislation. The e-administration have been extended after the reforms of 2014/2015 and it has been strengthened by the new legislation in 2023/2024. This regulatory framework and it major elements will be analysed by our chapter. As part of this examination, it should be emphasised, that the digital services are linked to Artificial Intelligence (AI) tools. However, compared to the business sector government sector has several specialties by which the application of AI is influenced. Therefore, these specialties and the possibilities of the use of AI by the Hungarian public administration is reviewed by our chapter.

Keywords: • digital services • digital citizenship • electronic administration • digitalisation • AI and public administration • Hungary

CORRESPONDENCE ADDRESS: Bertold Baranyi, Dr., Lecturer, Eötvös Loránd University, Faculty of Law, Department of Administrative Law, H-1053 Budapest, Egyetem tér 1-3., Hungary, e-mail: bertold.baranyi@baranyitimar.hu. András Bencsik, Ph.D., Dr., Habil., Associate Professor, Eötvös Loránd University, Faculty of Law, Department of Administrative Law, H-1053 Budapest, Egyetem tér 1-3., Hungary; Károli Gáspár University of the Reformed Church in Hungary, Faculty of Law, Department of Financial Law, H-1042 Budapest, Viola u. 2-4., Hungary, e-mail: bencsik.andras@ajk.elte.hu. István Hoffman, Ph.D., Prof. Dr., Full Professor, Eötvös Loránd University, Faculty of Law, Department of Administrative Law, H-1053 Budapest, Egyetem tér 1-3., Hungary; Maria Curie-Skłodowska University, Faculty of Law and Administration, Department of International Public Law, Plac Marii Curie-Skkodowskiej 5, 20-400 Lublin, Poland; Centre for Social Sciences, Institute for Legal Studies, H-1097 Budapest, Tóth Kálmán u. 2-4., Hungary, ORCID: 0000-0002-6394-1516, e-mail: hoffman.istvan@ajk.elte.hu.

https://doi.org/10.4335/2026.1.2 ISBN 978-961-7124-29-3 (PDF)
Available online at http://www.lex-localis.press.

1 Introduction

Today, the digital revolution has also caught up with the administration. E-governance has many advantages. For example, clients are not tied to office hours, do not have to meet with officers, they can access information more easily, and many tools are available to help them make decisions (Bowman & Kearney, 2016: 223). The *e-government* is an umbrella term (Gaie & Karpiuk, 2024: 176-178): it covers the government innovation and the government information and services – according to the relevant literature. The aim of e-government is oftenreferred as the paperless office, which means that electronic administration converts paper processes into electronic processes (Czuryk, 2023: 46). E-government creates a lot of ways that governments and citizens can communicate with each other. As a result, clients become the actors of the administrative system (Wohlers, 2010: 89-90).

The e-services are different, and the different stages of e-administration is distinguished. Four main stages of the e-government development are distinguished. This classification is based on the integration of the different services and on the complexity of the structures and technology. The first stage is the *catalogue*, in which the online presence of the government is provided, the main tasks are catalogued, and the several forms could be downloaded. The second stage is the *transaction*, in which the services and forms are online, and the online transactions are supported by several working databases. The third stage is the *vertical integration*, in which the local systems are linked to higher systems (within similar functionalities). The fourth stage is the *horizontal integration*, in which the systems with different functions are integrated and a real one-stop-shop is provided (Layne and Lee, 2001: 124-125).

It is highlighted by the literature, that significant investments are required to fulfil these aims, and the costs of these investments are partly related to the cybersecurity issues (Heeks, 2006: 107). But the e-government technologies have several prerequisites. After Layne and Lee three vital condition should be fulfilled to implement a successful e-government reform: universal access to the e-government tools, the defence of privacy and confidentiality and – last but not least – the citizen focus in government management. (Hoffman & Cseh, 2020: 200-202). Our chapter will be based on the analysis of the legal framework of this system.

The analysis of the digital public services and electronic administration has been based on the methods of jurisprudence because the regulatory environment of this phenomena has been analysed. Our chapter focuses on the analysis of the regulation, and it focuses on the analysis of the legal norms, soft law documents and partly the policy papers. Because these issues have a limited judicial practice, therefore, the judgements are just narrowly reviewed by our chapter (Evans et al. 2015).

The major challenges and results of the transformation of the regulation have been summarised by the chapter, as well. The primarily impact of the reforms and the application of AI on the government sector has been similarly analysed by the chapter.

2 Regulatory framework

By the adoption of Act CIII of 2023 on the Digital State and Certain Rules for the Provision of Digital Services (hereinafter: DCA), a *horizontal approach* was established, similar to Act CCXXII of 2015 on electronic administration (EAA) (Baranyi et al., 2018: 35-37), by which this area was previously regulated. In terms of its position in the legal system, it has similarities with Act CL of 2016 on the Code on General Administrative Procedure (CGAP).

Each procedural code may lay down different or additional rules on electronic administration to the general rules of the DCA, within the scope set out therein (Baranyi, 2018: 235). The CGAP, in line with its regulatory logic, contains few rules on e-government, while Act I of 2017 on the Code of Administrative Court Procedure (CACP), although providing for some rules, basically refers back to the rules of the Act CXXX of 2016 on Code on Civil Procedure (CCP). Different or additional detailed rules on electronic case management may be laid down in sectoral legislation within the scope of the DCA or the procedural codes.

The general rules for electronic administration are detailed in government regulations implementing the DCA. The DCA does not only regulate the electronic administration of administrative procedures, including those of administrative authorities. Under the Act, its provisions on e-government apply to the electronic handling of matters with customers by bodies providing digital services.

The scope of the *organisations providing digital services* is very broadly defined in the law. In addition to the bodies listed in detail, all legal entities authorised by law or government decree to exercise the powers of an administrative authority are also covered by the Act. The only public authorities excluded are those bodies which are statutory bodies of local government, unless they voluntarily undertake to provide electronic administration. Any legal entity, whether private or not, may voluntarily undertake to provide a digital service for the management of any matter, whether social or economic, which is not contrary to public morality. In return, they become entitled, under certain conditions, to use the services and tools available to the bodies responsible for providing mandatory eGovernment services.

The law also defines the scope of *clients* very broadly. In electronic administrative proceedings, the client is not only the client under the CGAP, but also other participants in the proceedings, i.e. the witness, the official witness, the expert, the interpreter, the holder of the object of inspection and the representative of the client. Accordingly, the

rights and obligations associated with electronic administration of the case are also vested in and imposed on these participants to the proceedings. The rules of the Eüsztv. relating to the client shall also apply in cases in which the body providing electronic administration participates as client, witness, interpreter or expert, and, mutatis mutandis, in administrative proceedings.

The DCA also defines the scope of *cases and jurisdiction* broadly. It covers not only administrative proceedings, but all public authority proceedings falling within the competence of an e-government body, and even matters relating to services provided by an e-government body under the law, such as the use or cancellation of public services, simply on the basis that the e-government body provides these services. It is up to the legal entities that voluntarily undertake eGovernment to determine the matters for which they undertake eGovernment.

3 Principles of electronic administration

In addition to the general principles of the legal system as a whole (i.e. good faith, fairness, mutual cooperation, proper administration of justice, protection of personal data, public interest and public disclosure of data of public interest), the DCA also sets out *specific* principles that are enforceable and even directly invocable: 1) *the right to electronic administration* is the fundamental basis of all client rights related to electronic administration; 2) the essential content of the *principle of technological neutrality* is that clients may choose any suitable means and solution for electronic administration and, in particular, they may not be obliged to use any means or IT system which entails additional costs; 3) *the principle of electronisation of the entire administrative process* means that electronic administration should not be designed by replacing some elements of traditional administration with their electronic counterparts, but by re-optimising the entire administrative process in the light of modern ICT solutions; 4) *presumption of lawful use of electronic* means of communication and means of electronic communication defined by the legal regulation: a) on the one hand, it creates a presumption that the customer is acting lawfully if he or she is contacting you in the manner and by the means specified in the law, b) on the other hand, the customer shall be deemed to be making lawful use of the means and means of contact specified, unless proven otherwise; 5) *the principle of positive discrimination in favour of electronic administration* in order to promote the application of electronic administration allows, for example, that the body providing digital services undertakes to take a decision sooner than the legal deadline in the case of electronic administration.

4 Digital citizenship and right to electronic administration – and its limitations

The obligation to provide e-government as part of digital services is seen as an entitlement to e-government on the client's side, which can also be seen as part of digital citizenship. The right to e-government, as the mother of procedural rights of the client, is not unlimited, as are other rights. *The most important limitations are defined are set by the DCA itself:* 1) a natural limitation of electronic administration is when it is not meaningful for the procedural act in question. Obviously, for example, a forensic expert cannot take a blood sample electronically, nor can a case be sealed electronically; 2) some of the rights of the detained person, including the right to electronic administration, may naturally be restricted to the extent strictly necessary for the execution of the sentence, measure or coercive measure; 3) the rules of the Act on the Protection of Classified Data do not apply to classified data, the electronic transmission of such data is only possible if the requirements set out in Act CLV of 2009 on the Protection of Classified Data are met; 4) where this is precluded by an international treaty or a directly applicable binding act of the European Union of general application, electronic administration shall not be used, mutatis mutandis, for any procedure or procedural act.

In addition to the following general conditions, electronic communication *may also be excluded by law or by government decree* under the original legislative power: 1) the exclusion of electronic administration may only apply to procedural acts, not to complete cases or groups of cases; 2) electronic administration may be excluded for a given procedural step only if the performance of the procedural step requires the submission of a document by means other than electronic means or the personal appearance of the client; 3) the non-electronic presentation of the document or the personal appearance of the client cannot be replaced or substituted by any other means.

5 The obligation of electronic administration and the consequences of failure of the fulfilment of the above-mentioned obligation

Entities obliged to participate in eGovernment. The DCA requires three categories of clients to apply electronic administration as a digital service. The first group includes business entities, which are defined in Article 7(6) of the CCP. Public entities, such as the State, municipalities, budgetary bodies, public prosecutors, notaries, public bodies and all other public authorities, are also obliged to administer their affairs electronically as customers. The third group of clients subject to the e-administration obligation includes legal representatives (attorneys at law, legal counsellors). The DCA includes in the definition of legal representative, on a subsidiary basis, a lawyer, law firm or attorney at law (including European Community lawyers and European Community law firms) acting on behalf of a client. These representatives are considered legal representatives even if legal representation is not mandatory in the public procedure. However, a lawyer, law firm or barrister cannot be considered to be legally represented if he is not acting as

a representative but is acting in his own interest. Accordingly, a law firm (as a business entity) is obliged to conduct its own affairs electronically, whereas an individual lawyer and a barrister are not.

In addition to the above, compulsory electronic administration *can be exclusively made mandatory by an Act of Parliament.*

Exceptions to mandatory electronic administration. Just as a client is not entitled to electronically administer a procedural step for which electronic administration is not meaningful; he is by analogy not obliged to do so for such a procedural step. Although there is an obligation to administer a case electronically, the legal consequences of failure to do so do not apply where the client or legal representative who is obliged to administer the case electronically does not do so because: 1) the body responsible for providing electronic administration does not comply with this obligation; 2) the necessary electronic administration or other services are not available; 3) the statutory form cannot be accessed electronically due to the failure of the body providing electronic administration.

Consequences of failing to comply with the mandatory electronic administration. The DCA sets out the legal consequences of failure to comply with the statutory obligation to administer public affairs electronically, i.e. by using non-electronic or inappropriate electronic means, in a subsidiary but general way, including in relation to administrative procedures and administrative litigation. Such *procedural acts are null and void*, i.e. they have no legal effect. The body providing digital services does not incur any obligation as a result of such an act of administration and does not take it into account in the administration of the case. A client who has not carried out a procedural act by electronic means, despite being obliged to do so, fails to comply with the time limit laid down by law or the body responsible for the procedure.

The DCA allows for the possibility of imposing *a different legal consequence* for failure to comply with the electronic filing requirement. The CGAP does not avail itself of this option. In administrative proceedings, failure to file an application or appeal electronically is not a case of ineffectiveness, but of *refusal.*

6 Rights and obligations of the clients. Obligations of bodies providing digital services

The right to digital services is an obligation on the side of the body providing digital government services, and client obligations often generate obligations on the side of the body acting. It is therefore worth considering them together, as distinct from the legal division.

Electronic identification. Although not all electronic transactions necessarily require the identification of the customer, this is unavoidable in administrative procedures and in

administrative litigation. The body providing digital services must ensure that, at least at the choice of the customer: 1) by means of an electronic administration service provided by the Government [for example, by means of a (new type of) ID card with a storage element], by means of a client gateway identification or by means of a so-called partial code telephone identification; 2) by means of an electronic identification service mutually recognised by Member States pursuant to Article 6 of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (this ensures interoperability between the electronic administration systems of the Member States) identify yourself.

Prohibition of data verification. The main driver for IT cooperation between e-government bodies is that they should obtain the information (data and documents) they hold electronically from each other and not from the customer. The customer has the right to choose whether or not to provide this available information in the course of the administration of the case, except, of course, for the data necessary for his identification. Which data can be obtained from which digital service provider body is indicated in the register of information sources.

Closely related to this is the obligation for the body providing electronic administration to connect to the register in order to ensure the information self-determination of customers. The purpose of this register is to ensure interoperability between the identification codes used by the different bodies, so that each body only knows the data it can process. The service (and the law) also provides the possibility for the customer to identify himself by an identification code that the body is not authorised to manage.

Usability of a certified electronic copy. In order to remove obstacles to electronic administration, the client has the right to use a certified electronic copy made by an authorised person (such as a notary, a lawyer or, under certain conditions, the client himself) instead of the original document, which must be accepted by the body providing electronic administration. Exceptions to this rule are: 1) electronic administration is excluded; 2) it is otherwise expressly excluded by law or government regulation; 3) if the original deed is invalid or has been revoked for any other reason (in which case the original deed cannot be used).

The body providing digital services may require the original document to be produced in case of doubt.

The client's right of disposal. The DCA's basic idea is to provide the widest possible range of electronic means of electronic administration, or even to develop them on a market basis, from which the customer can choose the most appropriate one according to his/her individual interests and life situation. This is reflected in the *concept of digital citizenship* as defined by the DCA. The right of choice is therefore about the right to choose, where,

for some overriding reason, the means of administration is not defined or limited by law, the means of administration available (including the means of carrying out each act of administration), as long as this right is not abused. In order to ensure that the customer's administrative arrangements are known and taken into account by the digital service providers, a so-called *register of arrangements* made electronically, in person or even by telephone is kept, which the digital service providers are obliged to take into account.

Among other things, the customer *may have the right to:* 1) a choice between electronic and non-electronic administration; 2) a choice of electronic means of administration (including means of identification); 3) the provisions governing the representation of the client (e.g. power of attorney); 4) notification of official electronic contact details.

Electronic information and payment. The clients have the right to be informed electronically or non-electronically about the electronic handling of the case, and even to be informed digitally about the non-electronic handling of the case. The digital services cannot be complete if the payment obligations related to the procedure (fees, administrative service charges, advance costs, etc.) cannot be executed electronically. Under the DAC, the business entity is obliged to make all payments electronically as a customer, and all other customers are, as a general rule, entitled to do so. Electronic payments can be made by bank transfer, simplified electronic payment or by credit card. To facilitate electronic payments, the Government operates an electronic payment and clearing system.

7 Rules on digital communication

Administrative procedures and administrative litigation can be described as a set of procedural acts. These procedural acts are, to a large extent, the declarations of the parties to the proceedings. Electronic communication is the making of statements by electronic means between the body providing electronic administration and the client. Accordingly, one of the most important elements of the right to electronic administration is that the client is entitled, and the digital service provider is obliged, if the client so decides, to make his or her statements electronically.

Choosing how to contact you. The choice between electronic and non-electronic means of communication, and between the different electronic means of communication, should be based on the following principles: 1) if an Act of Parliament specifies the method of contact, that method of contact shall apply; 2) where the law does not specify the means of contact or where several means of contact may be used, the client may choose either to be contacted in a simple manner or to specify this in the administrative provision; 3) if the customer and the law do not specify the means of communication, the digital service provider shall choose one of the possible means of communication.

However, the right to vote is not unlimited, it can only be exercised in good faith and in the proper exercise of the right, and the administrative authority is also bound by the requirement of a cost-effective procedure.

Submission of applications. In principle, the general rules on communication in the CGAP do not limit the electronic means of communication that may be used, but according to Section 35 (2) of the Public Act, applications may only be submitted in writing or in person, unless otherwise provided by law or government decree. Accordingly, requests may only be submitted by the client in written form, i.e. by electronic means that ensure the identification of the declarant and the integrity of the electronic document delivered. In addition, many laws require the use of an electronic form. For example, in administrative proceedings, statements of claim and other pleadings may be submitted electronically using a form only.

Communication and publication of the decision and other official documents. Likewise, any means of contact for the communication of an administrative decision or other official document may not be used.

In the case of written communication, the decision may only be notified by the electronic means referred to above, which are considered to be written. The CGAP also allows for oral communication of the decision, which is equivalent to communication by electronic means that ensure voice communication (e.g. by telephone or voip service). The restriction is that the administrative authority must either record the conversation or send a summary of it to the client, and the oral communication has the legal effect of communication only if the client does not object within 3 working days of receipt.

In administrative court proceedings, if the statement of claim is not served on the defendant, it is served on the defendant whose electronic contact details are not known on paper and the court invites the defendant to contact him or her electronically.

Official electronic contact. Electronic communication requires that both the customer and the administrative body have an official electronic contact address suitable for electronic communication. Such contact details shall be a so-called secure delivery service address or other contact details which, in a manner necessary to ascertain the legal effects of service, ensure: 1) that the message can only be received by the authorised person; 2) proof of successful or unsuccessful delivery and the date of delivery; 3) the integrity of the message delivered.

Business organisations, as they are obliged to administer their affairs electronically, are obliged to maintain official electronic contact details and register them in the register of provisions, while natural persons are in principle only able to do so but cannot communicate electronically without them.

For delivery to an official electronic contact, DCA will switch to a delivery fiction: 1) the consignment is deemed to have been delivered on the certified date of receipt; 2) if the addressee refuses to accept the delivery of a consignment received at the official contact address, the legal effect (fiction) of delivery is attached to the certified date of refusal; 3) there is a delivery fiction even if the consignee business entity does not receive the consignment at the certified time of the second notification, despite a second notification to that effect having been made to the official contact details.

If an economic operator does not have an official electronic contact, despite the legal obligation of the client, the official documents generated in the procedure must be served on paper, at the same time a legal compliance procedure must be initiated against the operator, and in administrative proceedings a procedural fine must be imposed on the operator (Csatlós, 2024: 191-193).

8 The role of artificial intelligence in Hungarian public administration

The public administration (including its organisational structure, its operational mechanisms and its staffing framework) does not (or cannot) remain unchanged, cannot be independent of the trends of the contemporary world, and thus it can be said that public administration is constantly in flux.

IT solutions (also) used in AI-based public administrations have shown varying degrees of effectiveness in different developed countries (Mezei & Träger, 2025: 144-146). Looking at examples from abroad, it can be highlighted that both machine learning and the use of expert systems are not alien at international level, with the Anglo-Saxon countries in particular leading the way in this field. Machine learning is the basis for the OPSI and BIT technologies, among others, which have been in existence since 2017, while examples of successful use of expert systems can be found in the UK (ESI), Australia (IVAG), New Zealand (CSLC) and the US (e-HASP2).

In addition to the need to keep up with technological advances, it is also evident that the challenges of recent years (e.g. pandemics, war, restrictions on fundamental rights, etc.) have forced public administrations to proactively exploit these existing infrastructures. An example of this in the Hungarian documentary administration is the effort to reinforce the so-called customer call kiosks in the district offices with artificial intelligence, which, at least according to plans, will in the near future enable the online initiation and issuance of documents of a decision nature (e.g. identity card, proof of address, driving licence, passport, etc.) without the involvement of human beings.

The other aspiration that pervades the domestic related legislation is to use artificial intelligence as (one of) the means to shorten the administrative time. To illustrate this, one can cite the automatic decision making institutionalised by the former Administrative Procedure Act and further developed by the Act CL of 2016 on the Code of General

Administrative Procedure (hereinafter: CGAP). The basic idea is that a decision is taken or communicated within 24 hours of the initiation of the procedure, provided that the facts are clear and the necessary information is available to the authority. It should be mentioned that the sectoral legislation was originally modelled on ex officio procedures for certain traffic offences, but was later extended to procedures on request and to other sectors (e.g. certain family allowances, the issue of an inauthentic title deed, etc.). The scope of this chapter does not allow for a comprehensive evaluation of this legal instrument established by the CGAP, so we would just like to add that – according to the conceptual coordinate system of the GDPR regulation – this cannot be considered as a real automated decision, since under the current regulation, the human factor is required to intervene approvingly to reach the actual decision (Wachter et al. 2018: 844-846). Similarly, this legal instrument cannot be considered as a pure application of artificial intelligence, even though the nature of the legislative act (i.e., the issuing of a legally binding act) would allow for the application of full automatism.

Finally, we would like to emphasise, in addition to the classical public authority activities, there is also the possibility of using AI in the context of public service organisation (once the guaranteed framework is in place). Examples of possible sectors include the organisation of public transport (which could be based on the operating mechanisms of Uber's existing platform) and the linking of so-called basic registers with administrative planning (e.g., birth registers could be used to draw automated conclusions from the number of children born in a municipality in order to plan the number of places in nurseries and kindergartens).

As a conclusion, the benefits of digitalisation of public administration (in this context, the use of artificial intelligence) in terms of increasing efficiency or reducing administrative costs are undisputed, but it should also be stressed that bringing the administrative location closer to the citizen has not resulted in the decentralisation of tasks and competences. On the contrary, the digitalisation of public administration has reinforced the principle of centralisation, so that the cautious rise of AI in Hungary can be identified with the process of centralisation (Bencsik, 2024: 14-16).

9 Conclusions

The digitalisation and the e-administration are important issues of the public administration reforms of the last decades. The challenges of the new, digital ages resulted the transformation of the traditional administration. As we reviewed, the Hungarian regulation on eGovernment and on the digitalisation of the public administration transformed significantly. The regulation was focused on the development a horizontally integrated e-administration. Following the 2013-2015 reforms the new act, the DCA establishes a framework for the electronic and digital public administration services.

Chapter III

Legal Bases for the Operation of E-government in Poland

MIROSŁAW KARPIUK & JAROSŁAW KOSTRUBIEC

Abstract The processing of cases by the public administration electronically is now a standard, not the future, although there is still a lot to do in this regard. Today it is difficult to imagine a public administration detached from the digital sphere. Modern administration is an e-government using new technologies to carry out the tasks assigned by the legislature. Particular attention should be paid to the process of informatization of the activities of bodies performing public tasks, including the need to adapt the ICT systems used to carry out such tasks, which should be highly resistant to interference. An important element in the functioning of such administration is also the exchange of information by electronic means, including electronic documents, between public entities and other actors, including citizens for whom e-government operates. In addition to the informatization of public administration activities, attention should also be paid to its digital accessibility, support for the development of telecommunications services and networks, including in the area of local government, the tasks of the Minister responsible for informatization, administrative e-proceedings, or cybersecurity issues. All these elements determine the status of e-government as a tool for meeting social needs.

Keywords: • e-government • information systems • informatization • cybersecurity

CORRESPONDENCE ADDRESS: Mirosław Karpiuk, Ph.D., Prof. Dr. Habil., Full Professor, University of Warmia and Mazury in Olsztyn, Faculty of Law and Administration, Department of Administrative Law and Security Sciences, ul. Obitza 1, 10-725 Olsztyn, Poland, ORCID: 0000-0001-7012-8999, e-mail: miroslaw.karpiuk@uwm.edu.pl. Jarosław Kostrubiec, Ph.D., Dr. Habil. Associate Professor, Maria CurieSkłodowska University (Lublin), Faculty of Law and Administration, Plac Marii Curie-Skłodowskiej 5, 20-031 Lublin, Poland, ORCID: 0000-0003-1379-9846, e-mail: jaroslaw.kostrubiec@mail.umcs.pl.

https://doi.org/10.4335/2026.1.3 ISBN 978-961-7124-29-3 (PDF)
Available online at http://www.lex-localis.press.

1 Introduction

In the age of information society and digital government, public administration has faced new challenges to adapt not only to the requirements of a modern governance, but also to the needs of the information society, including communication with office personnel via the Internet. Remote handling of cases should not be an exception but rather, on the contrary, the standard of operation of the public administration enabling stakeholders to contact quickly, without having to appear in the office in person.

An efficient and open public administration is where the state's organisational and management system is characterised by a high quality of public services, internal computerisation and professionalism. The degree of openness of the public administration is also evidenced by the digital competences of the society (Karpiuk, Chałubińska-Jentkiewicz, 2015a: 102). The digital society forces the administration to switch from a conventional model to an electronic model, where most public services are provided electronically. However, the digitally excluded must be still taken into account, as they must also have access to the services provided by the public administration.

The solutions being implemented for the functioning of modern e-government ensure the provision of e-services through different ICT platforms. The emerging opportunities for the development of this sphere of public life inevitably face various problems and barriers (Romaniuk, 2022: 464). Electronic exchange of services in the global economy is becoming increasingly important, but giving rise to previously unknown risks. This phenomenon is linked to the ever-increasing exchange of information and the emergence of goods and services that can be purchased through ICT networks (Karpiuk, Chałubińska-Jentkiewicz, 2015b: 121).

Owing to information systems, the e-government has new capabilities to be employed to perform public tasks, but it is still important to ensure that appropriate safeguards are applied when using these systems so that disruptions do not compromise the continuity and quality of these tasks.

In an era when information systems form the foundation of many areas of public life, or are an instrument supporting public activities, they both need to respond to the dynamics of change and be properly protected (Karpiuk, 2023: 50). The development of new technologies indeed contributes to streamlining the provision of public services, but also makes cyber threats more and more dangerous. Therefore, information systems used by public administrations must be more resilient to cyberattacks restricting access to services provided through them.

2 Informatization of the activity of public administration

Informatization is not only a dynamic, but also continuous and indispensable process. It is nowadays impossible to govern correctly without a properly developed IT infrastructure, which is very important for the operation of public administration. Widespread informatization covers the public sector, which must operate effectively, efficiently, quickly and fairly, reaching the widest possible range of beneficiaries. It is a process that allows an improvement of the implementation of public tasks, or a wider access to information, while reducing the costs of public administration operation (Chałubińska-Jentkiewicz, Karpiuk, 2015: 425).

As stated in Article 13 of the Act of 17 February 2005 on informatization of the activities of entities performing public tasks (consolidated text Journal of Laws of 2023, item 57 as amended), – hereinafter referred to as the Informatization Act, the public entity uses for the performance of the public tasks ICT systems which meet the minimum requirements provided for these systems, including ensuring their interoperability, while ICT systems used for scientific and educational purposes do not have to meet these requirements. The ICT system is defined in Article 3(3) of the Informatization Act as a set of interoperating IT hardware and software ensuring the processing, storage, transmission and reception of data by telecommunications networks using a terminal equipment appropriate for a given type of telecommunications network, thus, as follows from Article 2(43) of the Act of 16 July 2004. Telecommunications Law (consolidated text Journal of Laws of 2022, item 1648 as amended), - telecommunication equipment to be connected directly or indirectly to network terminations. The minimum requirements for ICT systems, according to Article 3 (9) of the Informatization Act, are a set of organizational and technical requirements, the fulfilment of which by the ICT system used for the performance of public tasks enables the exchange of data with other ICT systems used for the performance of public tasks and ensures access to the information resources made available by these systems. Interoperability, on the other hand, is, as defined in Article 3(18) of the Informatization Act, the ability of various entities and ICT systems and public registers used by them to cooperate in order to achieve mutually beneficial and agreed objectives, taking into account the sharing of information and knowledge by the business processes supported by them and implemented using data exchange through the ICT systems used by those entities.

Interoperability – according to § 4 of the Ordinance of the Council of Ministers of 12 April 2012 on the National Interoperability Framework, minimum requirements for public registers and exchange of information in electronic form and minimum requirements for ICT systems (consolidated text Journal of Laws of 2017, item 2247) – is achieved by: 1) unification, understood as the use of compatible norms, standards and procedures by various entities performing public tasks, or 2) interchangeability, understood as the possibility of substituting a product, process or service without simultaneous interference with the exchange of information between entities performing

public tasks or between these entities and their customers, while meeting all the functional and non-functional requirements of the interoperating systems, or 3) compatibility, understood as the suitability of products, processes or services intended for joint use, under specific conditions ensuring the fulfilment of the relevant requirements and in the absence of undesired effects. The application of the above rules depends on the circumstances arising from the risk assessment and the characteristics of the ICT system being designed, its extent and the solutions available on the IT supplies and services market. It should be emphasised, however, that the way in which interoperability is achieved by the entity performing public tasks must not breach the principle of technological neutrality.

A number of administrative entities maintain public registers, defined in Article 3(5) of the Informatization Act as registers, records, lists, inventories or other forms of records, serving the performance of public tasks, maintained by a public entity. The public entity is obliged to: 1) maintain the register in a manner that ensures that the minimum requirements for ICT systems are met, where the register operates using ICT systems; 2) maintain the register in accordance with the minimum requirements for public registers and the exchange of information in electronic form; 3) enable information to be provided to this register and information from this register to be made available electronically, where the register operates using ICT systems. This obligation stems from Article 14 of the Informatization Act. Keeping records of various aspects of the public administration's operation facilitates considerably the performance of its tasks and enables direct access to the database it holds, which also applies to sharing the information contained therein.

According to Article 15 of the Informatization Act, an entity maintaining a public register shall provide a public entity or a non-public entity carrying out public tasks with free access to the data collected in the register, to the extent necessary for the performance of those tasks. These data should be made available by electronic means and used for the performance of public tasks. A means of electronic communication is understood in Article 2(5) of the Act of 18 July 2002 on the provision of services by electronic means (consolidated text Journal of laws of 2020, item 344 as amended) as technical solutions, including ICT equipment and software tools interoperating with them, enabling individual distance communication using data transmission between ICT systems, including in particular e-mail.

The request for access to the data collected in the register – as is apparent from § 2 of the Ordinance of the Council of Ministers of 27 September 2005 (consolidated text Journal of laws of 2018, item 29) – contains: 1. the name of the entity requesting access to the data collected in the register and the address of its office; 2. the name of the requested entity; 3. the identification of the register in which the data to be made available are collected; 4. specification of the public task and the legal basis for its performance by the entity requesting access to the data stored in the register, the performance of which requires that the data be made available; 5. specification of the extent of the data requested

and the manner in which it is made available; 6. specification of the period during which the data are made available; 7. a declaration of the entity applying for access to the data collected in the register that the data will be used exclusively for the performance of a public task; 8. a statement of compliance by the entity requesting access to the data stored in the register with the technical and organisational security conditions necessary for access to that data; 9. the personal signature or qualified electronic signature of the representative of the entity requesting access to the data collected in the register.

When providing information from the register for its further use for purposes other than the performance of a public task, the entity maintaining a public register (as an entity obliged to provide or transmit public sector information for multiple use) shall not restrict the use of that information by other users. This principle of non-discrimination follows from Article 9(1) of the Act of 11 August 2021 on open data and further use of public sector information (Journal of Laws of 2021, item 1641 as amended). The President of the Council of Ministers may entrust the entities obliged to share or transmit public sector information for further use with tasks in the field of public sector informatization, digital innovation and development of information society and countering digital exclusion, as provided for in Article 10c (1) of the Act of 8 August 1996 on the Council of Ministers (consolidated text Journal of Laws of 2021, item 178 as amended). This is intended to promote the development of the digital society as well as to shape digital awareness in citizens, including sensitizing them to cyber threats, including promoting knowledge about the safe use of ICT systems (Karpiuk, 2022a: 18).

When organizing data processing in the electronic system , the public entity – pursuant to Art. 16(1) of the Informatization Act – is obliged to ensure that data can also be transmitted in electronic form by exchanging electronic documents related to handling of cases falling within its scope of activity, using IT data carriers or electronic means of communication.

The public entity shall inform on its pages of the Public Information Bulletin about: 1) the address of the electronic registry inbox provided in the form of a URI; 2) the maximum size of the electronic document with its attachments, expressed in megabytes, which can be served by means of the electronic registry inbox, not less than 5 megabytes; 3) the scope of electronic documents created using templates placed by these entities in the central repository or the repository of electronic document templates; 4) the types of electronic data carriers on which an electronic document can be served; 5) the types of electronic data carriers on which an official confirmation of receipt can be stored; 6) other legal requirements for the service of electronic documents. The legislature introduces this information obligation in § 3 of the Ordinance of the President of the Council of Ministers of 14 September 2011 on the drawing up and service of electronic documents and the provision of forms, templates and copies of electronic documents (consolidated text Journal of Laws of 2018, item180).

An important aspect of improving the quality of e-government is auditing. The scope of these audits is defined in Article 25 of the Informatization Act and Justice as follows: 1) the audit of the implementation of cross-sectoral IT projects is carried out by the President of the Council of Ministers; 2) the audit of the implementation of sectoral IT projects is carried out by the minister in charge of the central government administration department for which a sectoral IT project has been established; 3) the audit of the operation of ICT systems used for the performance of public tasks or the following duties: meeting the requirement of equal treatment of IT solutions of the ICT system used for data exchange; publication in the Public Information Bulletin or otherwise making available the list of electronic documents structures, data formats, communication and encryption protocols, as well as well as acceptance tests – shall be carried out: a) in local government units and their associations, as well as legal entities and other local government organisational entities created or run by these local government units – the competent provincial governor (*wojewoda*), b) in public entities subordinated or supervised by the central government administration – the administration body of central government supervising the public entity, c) in other public entities - the minister responsible for informatization. The audit is carried out in terms of compliance with minimum requirements for electronic systems or minimum requirements for public registers and electronic information exchange. In the case of local government and entities established by them, the audit may only concern electronic systems and public registers which are used for the performance of central-government tasks entrusted to the local government. If an assessment of another electronic system or public register is necessary to obtain a full assessment of the electronic system or public register used for the performance of central-government tasks entrusted to the local government, that particular system or register may also be subject to the audit. Audits on the regularity of the spending by local government units and their associations, as well as legal persons and other local government organisational units established or operated by these local government units of funds provided in the form of a special purpose grant – from the point of view of legality, cost-effectiveness, purpose and reliability of public spending – are carried out by the competent chamber of audit. Regional chambers of audit are the state financial supervision and audit bodies. This status is determined in Article 1(1) of the Act of 7 October 1992 on Regional Chambers of Audit (consolidated text Journal of Laws of 2022, item 1668 as amended).

The conduct of an audit – as follows from Article 3 of the Act of 15 July 2011 on audit in the central government administration (consolidated text Journal of Laws of 2020, item 224 as amended), – aims to evaluate the activities of the audited entity based on established facts and with the use of adopted criteria of audit. Where irregularities are found, the purpose of the audit is also to establish their extent, causes and consequences and the persons responsible, and to make recommendations with a view to remedying the irregularity.

3 Digital accessibility of public administration

Public entities are required to guarantee digital accessibility, and therefore the operation of websites or mobile applications, by ensuring their functionality, compatibility, visibility and comprehensibility. This obligation results from Article 5 of the Act of 4 April 2019 on the digital accessibility of websites and mobile applications of public entities (consolidated text Journal of Laws of 2023, item 82 as amended) hereafter ADA. The website is defined in Article 4(10) ADA as a set of logically arranged elements, linked together by navigation and links, presented using a web browser under a single web address; and the mobile application, is defined in Article 4(1) ADA as a publicly accessible software with a touch interface designed for use on portable electronic devices, excluding applications intended for use on portable personal computers. According to the legislature, functionality is the property of a website or mobile application enabling the user to use all the features offered by it (Article 4 (4) ADA), compatibility is the property enabling this website or application to interoperate with as many computer programmes as possible, including tools and software supporting disabled persons (Article 4 (6) ADA), visibility – the property of a website or mobile application enabling it to be received by the user through hearing, sight or touch (Article 4 (9) ADA), and comprehensibility is a property enabling the user of these webpages and applications to understand the content and the manner of their presentation (Article 4(11) ADA)

The Minister responsible for informatization, as part of supervision exercised over the application of ADA regulations by public entities, submits inquiries to these entities in digital accessibility matters, in particular about the number and method of settling complaints about ensuring the availability of the digital website, mobile application or elements of the website or mobile application. The minister may also impose fines, by way of an administrative decision, on public entities in matters relating to digital accessibility. The extent of this supervision is defined in Article 13 ADA.

Based on the information contained in the declarations of availability, the minister responsible for computerization draws up a list of mobile applications of public entities and the same minister, in cooperation with the Research and Academic Computer Network - National Research Institute (NASK), draws up a list of addresses of websites of public entities. The competence of the minister responsible for informatization in this regard is provided for in Article 14 ADA. As stated in § 2 of the Ordinance of the Council of Ministers of 7 June 2017 on granting the Research and Academic Computer Network the status of a national research institute (Journal of Laws of 2017, item 1193), the NASK's areas of activity include: 1) conducting research and development work in the fields of: a) telecommunication, b) ICT, c) cyber security, d) the operation of the Polish register of internet domains, f) information society; 2) adapting the results of research and development works to the needs of practice;3) implementation of R&D results in services provided for *inter alia*, security and law enforcement purposes, national security and the

security of critical infrastructure units. NASK runs the Computer Security Incident Response Team operating at the national level (CSIRT NASK).

4 Electronic delivery

The structure of the Act of 18 November 2020 on e-delivery (consolidated text Journal of Laws of 2022, item 569 as amended), – hereinafter AED, is based on two basic principles: the primacy of electronic delivery over ¬traditional delivery and the principle of universality of electronic delivery. The essence of the principle of the primacy of electronic delivery is the organisation of exchange¬ of correspondence essentially by means of a¬ public service of registered electronic delivery to an e-mail address. This electronic service is complemented by a hybrid¬ public service combining the characteristics of electronic delivery with the traditional handing a letter to the addressee in person. The hybrid public service is addressed to digitally excluded persons and those who, for reasons other than digital exclusion, are not yet ready to abandon the traditional method of delivery (Skóra, 2022: 474-475). As provided for in Article 5 AED, a public entity shall deliver correspondence requiring confirmation of its sending or receipt by means of a public hybrid service where: 1) it is not possible to send correspondence to an e-mail address or 2) the public entity is aware that a natural person having an e-mail address has been imprisoned.

Article 6 AED provides for the exemption of the application of the provisions on the address for electronic delivery and the use of the public hybrid service. According to that provision, those exemptions apply where: 1) the entity requests the delivery of a document originally drawn up in a hardcopy form 2) the correspondence may not be delivered to an e-mail address or through a hybrid public service because of: a) the inability to draw up and transmit a document in electronic form resulting from separate rules, b) the inability to use a hybrid public service resulting from special provisions, c) the need to deliver a non-transformable document recorded in a non-electronic form or a tangible object, d) an important public interest, in particular national security, defence or public order, e) technical and organisational constraints arising from the amount of correspondence and other reasons of technical nature; 3) special provisions provide for the possibility of delivery also by means other than a public electronic registered delivery service or hybrid public service, in particular by its employees, and the sender, in specific circumstances, considers another method of delivery to be more efficient.

The legislature, in Article 8 AED, obliges the public entity to have an address for electronic delivery entered in the electronic address database, linked to a public electronic registered delivery service The address for electronic delivery defined in Article 2(1) AED, is an electronic address (designation of the ICT system enabling communication by means of electronic communication, in particular electronic mail, Article 2(1) of the Act of 18 July 2002 on the provision of services by electronic means, consolidated text Journal of Laws of 2020, item 344 as amended), - of the entity using a public electronic

registered delivery service or hybrid public service or a qualified registered electronic delivery service, enabling the unambiguous identification of the sender or addressee of the data sent using these services.

An entity required to provide the public service of registered electronic delivery under Article 38 AED is the designated operator (the postal operator responsible for providing the universal service — Article 3(13) of the Act of 23 November 2012 Postal law, consolidated text Journal of Laws of 2022, item 896 as amended). The public electronic registered delivery service shall be provided: 1) in accordance with the standard covering: a) the technical requirements for the transmission of electronic documents as part of the public electronic registered delivery service, b) the manner of identification of the sender and the addressee of the data as part of the public electronic registered delivery service, c) the structure of dispatch confirmation and receipt confirmation as part of the public electronic registered delivery service, d) the form and method of issuing the dispatch confirmation, issuing the receipt confirmation, recording of the dispatch confirmation and receipt confirmation as part of the public electronic registered delivery service, e) the scope and structure of data related to communication between addresses for electronic delivery, f) the requirements of the functioning of the registered e-delivery inbox - Article 26a of the Act of 5 September 2016 on trust services and electronic identification, consolidated text Journal of Laws of 2021, item 1797 as amended; 2) at reasonable prices. The designated operator, when providing the public electronic registered delivery service, shall ensure: 1) the identification of the sender before the dispatch of the data; 2) the identification of the addressee before the delivery of the data; 3) securing the data dispatch and receipt by an advanced electronic seal in such a way that no undetectable alteration of the data is possible; 4) notifying the sender and the addressee of any change of data necessary for the purpose of sending or receiving the data; 5) the indication, by means of a qualified electronic timestamp, of the date and time of sending, receiving and any change of the data. Electronic registered delivery service means a service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations, Article 3 (36) of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, p. 73)

A designated operator is required to provide the public hybrid service pursuant to Article 45 AED. The public hybrid service shall be provided: 1) in a uniform manner under comparable conditions; 2) ensuring that post offices of the designated operator are deployed throughout the country; 3) in compliance with standard letter delivery times; 4) at affordable prices; 5) at a frequency ensuring the delivery of letters at least on each working day and not less than 5 days per week, excluding public holidays; 6) in such a way as to ensure that the sender receives an electronic document confirming receipt of

registered mail (mail accepted against receipt and delivered against receipt – Article 3 (23) of the Act of 23 November 2012 Postal law, consolidated text Journal of Laws of 2022, item 896 as amended). When providing a public hybrid service, the designated operator must ensure the operation of: 1) the infrastructure necessary for printing and enveloping the correspondence sent in an electronic form; 2) the postal network necessary for the sorting, shipment and delivery of mail. According to § 2 of the Ordinance of the Minister of State Assets of 9 August 2021 on the implementation of the public hybrid service domestically (Journal of laws of 2021, item 1503 as amended), the standard time of delivery of letters is up to 6 days from the date of posting the electronic document containing the contents of the correspondence transformed into a letter until the date of delivery, notification of attempt to deliver the letter, or refusal to accept the letter containing the correspondence.
The designated operator providing a public hybrid service is required, pursuant to Article 46(1) AED, to convert an electronic document sent by a public entity from an e-delivery address into a letter in order to deliver the correspondence to the addressee. The conversion takes place in an automated manner, ensuring the protection of postal secrecy at each stage of the service.

Reference should be made to the position of the Regional Administrative Court in Warsaw in its judgment of 23 April 2021, VII SA/WA 2392/20 (LEX No 3178567), according to which wrong proceeding by an administrative body regarding the adopted form of a document served by means of electronic communication must not harm the party who received such a document, including depriving that party of the right to appeal against the decision received in this way. The rules on delivery are, above all, a guarantee for the party to the proceedings and not for the body, and cannot be interpreted to the detriment of the party.

5 E-government and cybersecurity

The ICT systems used by the public administration must be adequately protected, preferably free from interference, but at least protected against interference that undermines their normal functioning and limits the quality of the provision of public services through such systems. Therefore, an adequate level of cybersecurity must be maintained in this area of public administration activity.

Cybersecurity is defined – by Article 2(4) of the Act of 5 July 2018 on the national cybersecurity system (consolidated text Journal of Laws of 2022, item 1863 as amended) hereafter ANCS – as the resilience of information systems to activities affecting the confidentiality, integrity, availability and authenticity of data processed or related services offered by these systems. Cybersecurity is a specific sector of security that includes the protection of information systems against threats (Czuryk, 2019: 42; Karpiuk, 2021a: 46-47; Karpiuk, 2021b: 234). It covers the threat prevention and

forecasting, as well as remedying the effects arising as a result of these threats (Karpiuk, 2021c: 612).

Ensuring security in cyberspace is one of the basic tasks of public authorities. Threats of an IT nature have increasingly serious consequences and cyber attacks can be used not only as a means of economic pressure but also political one (Kaczmarek, 2019: 145).

The Polish legislature determines the organisation of the national cybersecurity system, as well as the tasks and responsibilities of the entities which form part of the system. According to Article 3 ANCS, the aim of the national cybersecurity system is to ensure security in cyberspace at national level, including the undisturbed provision of essential services and digital services, by achieving an adequate level of security of information systems for the provision of these services and ensuring incident response. This is achieved, also in the case of e-government and its electronic services, through information systems (ICT systems together with electronic data processed therein). The national cybersecurity system consists of public entities of different legal and territorial status, as well as non-public entities. However, public entities, especially those specialised in cybersecurity, are essential to that system (Chałubińska-Jentkiewicz, Karpiuk, Kostrubiec, 2021: 4).

One of the authorities responsible for cybersecurity is the Minister of National Defence, who directs the section of national defence covering during peacetime the cybersecurity issues in the military dimension. The tasks of this central government administration body cover cybersecurity only in the military dimension. Cybersecurity issues in the civil dimension are covered by the section of informatization (Karpiuk, 2022b: 87). The Minister of National Defence is the governing body in the military sphere, including in matters of ensuring cybersecurity. It carries out tasks in this regard through subordinate and supervised organizational units (Bencsik, Karpiuk, 2023: 89). The body that is competent in the area of civil cybersecurity is the Minister responsible for informatization matters.

In the case of cybersecurity, an appropriate level of protection of information systems should be ensured, therefore, to guarantee that level, there may be restrictions on the freedoms and rights of individuals in cyberspace in specific cases. This is permissible provided that such protection is not otherwise assured (Czuryk, 2022a: 34). Security in cyberspace should be particularly protected, even in certain cases against individual freedoms and rights, if their exercise contradicts the need to ensure the cybersecurity of the state (Karpiuk, 2022d: 406).

Therefore, cybersecurity, as the resilience of information systems to disruptions, including with regard to data processed or services provided through them, must be adequately protected, accordingly to the threats. Such protection ensures the normal functioning of the public administration, which handles many matters electronically,

thereby greatly facilitating contact with the general public. In so doing, it shall make public services more efficient, swifter and more accessible to the citizen.

6 Supporting the development of telecommunication services and networks

Specific tasks in the area of supporting telecommunication services and networks have been assigned to local government as a structure that is closest to citizens. Pursuant to Article 3 of the Act of 7 May 2010 on the support for the development of telecommunications services and networks (consolidated text Journal of Laws of 2022, item 884 as amended) hereafter ASD, the local government body, in order to meet the collective needs of the local community, may: 1) build or operate telecommunications infrastructure and networks and acquire rights in telecommunications infrastructure and networks; 2) provide telecommunications networks or provide access to telecommunications infrastructure; 3) provide, using its telecommunications infrastructure and networks, services to specific entities (including telecommunications operators or end-users). Activities involving the construction of telecommunications infrastructure and networks may be undertaken if, in the area concerned: 1) there are no telecommunications infrastructure and networks; (2) existing telecommunications infrastructure and networks are not available or do not meet the needs of the local government unit.

Where that activity involves the provision by the local government unit of an internet access service through publicly available internet access points free of charge or for a fee lower than the market price, the information on the taking up of activities to support the development of telecommunications services and networks must also include the location of publicly available internet access points and an indication of the area where the service is provided through those points.

The local government unit may provide internet access services through publicly accessible internet access points free of charge or for a fee lower than the market price only in public places. According to § 1 of the Ordinance of the Minister of Informatization of 18 October 2018 on the minimum bit rate for Internet access services provided by local government units (Journal of Laws of 2018, item 2078) – the minimum bit rate for Internet access services provided by local government units via publicly available Internet access points free of charge or for a fee lower than the market price is 30 Mb/s.

The support for the development of telecommunications services and networks is provided in order to meet the collective needs of the local community. Public tasks serving to satisfy the needs of the local community, as stipulated in Article 166(1) of the Constitution of the Republic of Poland of 2 April 1997 (Journal of Laws of 1997, No. 78, item 483, as amended), are performed by the local government unit as its own tasks. These tasks are the basic tasks of the local government. They are placed at the appropriate level of local government by the constitutional principle of subsidiarity (Winczorek, 2008:

331). These tasks are territorial in nature, defined by the boundaries and level of the local government where the local government unit concerned operates, and should concern its inhabitants (Banaszak, 2009: 752).

Pursuant to Article 3a ASD, the executive body of the local government unit concerned may award to entities not included in the public finance sector and not engaged in a commercial business a special-purpose grant from the budget of the local government unit for the financing or co-financing of investment costs related to meeting the needs of those entities for access to the high-speed telecommunications network at the location of the end-user. As provided for in Article 126 of the Act of 27 August 2009 on public finance (consolidated text Journal of laws of 2022, item 1634 as amended) these grants are funds, subject to special accounting rules, from the state budget, local government unit's budget and State's special funds allocated under the Act, separate legislation or international agreements, for financing or co-financing the fulfilment of public tasks. The rules governing the award of a specific-purpose grant, including in particular the criteria for selecting projects for financing or co-financing and the procedure for awarding that grant and the method of accounting for it, are to be determined by a resolution adopted by the legislative body of the local government unit. Therefore, the legislature leaves the local government authorities a discretion in this regard. In the judgment of 16 April 2019, III SA/Po 9519 (LEX no 2654279), the Regional Administrative Court in Poznań states that each grant is intended to finance or co-finance the performance of public tasks, i.e. tasks that exist at the date of granting the right to finance or co-finance them. It is only when the right to the grant has been awarded that a public task can be implemented. The grant is a redistributive expense, for future purposes, and derogations, if any, must clearly stem from statutory provisions.

The local government unit, when entrusting a telecommunications company with the performance of activities in the field of supporting the development of telecommunications services and networks, where it is not possible, due to economic conditions, in a given area for the telecommunications company to carry out financially viable telecommunications business, may, pursuant to Article 8 ASD :1) provide telecommunications infrastructure or networks to the telecommunications company for fees lower than the cost of production; 2) co-finance the costs incurred for the provision of telecommunications services to end-users or telecommunications companies for the purpose of providing such services.

The issues concerning the activities of local government units to stimulate demand for services related to Internet access are set out in Article 15 ASD. According to that provision, local government units may take measures to stimulate or aggregate user demand for broadband internet services, in particular education and training services, by equipping consumers with telecommunication terminal equipment or computer equipment, or by financing the cost of telecommunications services borne by consumers. The legislative body of the local government unit determines, by resolution, the

conditions and procedure for financing that activity, in particular by determining the conditions of eligibility of the beneficiaries of the aid. The above activities are carried out in a non-discriminatory manner, with transparency and proportionality, and are aimed at maintaining technological neutrality. Any project undertaken by local government to stimulate demand for services related to Internet access requires prior publication, with a description thereof, in the Public Information Bulletin on the website of the local government unit concerned and at the office premises of that unit.

The legislature also introduced specific rules for the location of telecommunications projects. Pursuant to Article 46 ASD, the local spatial development plan may not establish prohibitions, and the solutions adopted therein may not prevent the location of public purpose projects in the field of public connectivity, if such a project is in compliance with special provisions. Public connectivity is defined in Article 4(18) of the Act of 21 August 1997 on real estate management (consolidated text Journal of Laws of 2021, item 1899, as amended) as telecommunications infrastructure serving to provide publicly available telecommunications services, therefore according to Article 2(31) of the Act of 16 July 2004. Telecommunications Law (consolidated text Journal of Laws of 2022, item 1648 as amended), – telecommunications services (services consisting primarily in the transmission of signals over a telecommunications network) available to the general public.

In the absence of a local spatial development plan, the location of a public connectivity project other than telecommunications infrastructure of little impact is determined by a decision on the location of a public-purpose project. The elements of the decision on the location of a public-purpose project are specified in Article 54 of the Act of 27 March 2003 on spatial planning and development (consolidated text Journal of Laws of 2022, item 503 as amended). According to this provision, the decision defines:1) the type of project; 2) the conditions and detailed rules for land planning and development resulting from special provisions, including in the area of : a) conditions and requirements for the protection and shaping the spatial order, b) protection of the environment and human health and cultural and historical heritage and works of contemporary culture, c) maintenance in terms of technical infrastructure and communication, d) requirements regarding protection of interests of third parties, e) protection of civil structures in mining areas; 3) lines demarcating the project site, delimited on the map on an appropriate scale. Such a decision must also meet the conditions laid down in Article 107 of the Act of 14 June 1960 Code of Administrative Procedure (consolidated text 2022 Journal of Laws, item 2000 as amended), hereinafter referred to as CAP, and thus contain the following elements: 1) identification of the public administration body; 2) date of issue; 3) identification of the party or parties; 4) reference to the legal basis of the decision; 5) ruling; 6) statement of factual and legal reasons; 7) instruction on whether and how the party may appeal against the decision and on the right to waive the appeal and the consequences of such waiver; 8) signature including the name and official position of the employee of the body authorized to issue the decision; 9) where the decision may be

appealed against by way of an action brought before common court, protest against decision or application to an administrative court – the instruction on the admissibility of filing the action, the protest against the decision or application and on the amount of the procedural fee if fixed, or on the basis of calculation of the fee if proportional, as well as the possibility for the party to apply for an exemption from procedural costs or granting legal aid. The factual reasons for the decision should in particular include an indication of the facts which the body has found to be proven, the evidence on which it relied and the reasons why other evidence has been found incredible and devoid of probative value, while the legal reasons should explain the legal basis for the decision, together with citing the relevant legal provisions. According to the position of the Regional Administrative Court in Gliwice expressed in the judgment of 12 April 2022, II SA/Gl 1500/21 (LEX nr 3338604), the minimum formal requirements of the decision are: the identification of the body which has issued it, the addressee of the decision, the content of the decision and the signature of the person who has issued it. The document does not have to be titled as a decision, but must contain a ruling.

The Regional Administrative Court in Poznań, in its judgment of 12 January 2022, II SA/Po 956/21 (LEX No. 3285590), stated that the decision on the location of a public purpose project was not enforceable due to its subject. Such a decision specifies only the type of project that can be carried out in a given area, the conditions and detailed rules for land planning and development resulting from separate regulations, as well as the lines demarcating the project area. Thus, such a decision does not have any substantive legal effects and does not give the investor the right to commence construction works related to the planned project.

7 Minister responsible for informatization and his responsibilities

The minister responsible for informatization is in charge of the section of informatization, and according to Article 12a of the Act of 4 September 1997 on central government administration sections (consolidated text Journal of Laws of 2022, item 2512, as amended), this section includes the matters of: 1) informatization of the public administration and entities performing public tasks; 2) ICT systems and networks of the public administration; 3) support for projects in the field of informatization; 4) implementation of the international obligations of the Republic of Poland in the field of informatization and telecommunication; 5) participation in shaping the European Union policy in the field of informatization; 6) development of the information society and counteracting digital exclusion; 7) development of services provided electronically; 8) shaping the national policy in the area of personal data protection; 9) telecommunications; 10) cyberspace security in the civil dimension; 11) the PESEL register, the Register of Personal Identity Cards, the Register of Civil Status and the Register of Passport Documents; 12) the register of vehicles, the register of drivers and the register of parking card holders; 13) supervision of the provision of trust services as defined in the

regulations on trust services; 14) electronic identification. The minister responsible for informatization supervises the President of the Office of Electronic Communications.

Under Article 19a of the Informatization Act, the minister responsible for informatization shall ensure the functioning of the Electronic Platform of Public Administration Services (ePUAP). H shall publish on that platform information on the addresses of electronic registry inboxes provided by public entities.

According to the position contained in the judgment of the Regional Administrative Court in Warsaw of 26 March 2021, VII SA/Wa 1959/20 (LEX No. 3173288), a precondition for granting an ePUAP functionality is not only the performance of public tasks, but having the status of a public entity. Pursuant to § 7 of the Ordinance of the Minister of Digital Affairs of 5 October 2016 on the scope and conditions of using the electronic platform of public administration services (consolidated text Journal of Laws of 2019, item 1969, as amended), a public entity shall apply to the minister responsible for informatization with a request to grant the functionality of a public entity on ePUAP. The application shall include the following elements: 1) identification of the public entity; 2) name and surname of the person authorized to represent the public entity together with the function or position; 3) details of the entity's administrator. The functionality of a public entity on ePUAP becomes available upon approval of the application by the minister.

Pursuant to Article 19b of the Informatization Act, the Minister responsible for informatization operates as part of the ePUAP a central repository of electronic document templates. Public administration bodies provide electronic document templates to the central repository and make them available in the Public Information Bulletin. International standards for preparing electronic documents by public administration bodies are used for the drafting of electronic documents, taking into account the need to sign them with a qualified electronic signature. The central repository for electronic document templates contains, stores and makes available document templates that take into account the necessary structural elements of electronic documents. The essential structural elements of electronic documents – as follows from § 2 (2) of the Ordinance of the Minister of Internal Affairs and Administration of 30 October 2006 on necessary structural elements of electronic documents (Journal of Laws of 2006, No. 206, item 1517 as amended)– are the following metadata: 1) identifier – a unique, in a given set of documents, tag of a document that enables its identification; 2) creator – the entity responsible for the content of the document, with specification of the creator's role in the process of document drafting or acceptance; 3) title – the name given to the document; 4) date – the date of the event related to document creation; 5) format – the name of the data format used to prepare the document; 6) access – identification of those to whom the document can be made available, under what rules, and to what extent; 7) type – determination of the basic document type (e.g. text, sound, image, video, collection) based on the list of types of the Dublin Core Metadata Initiative and its possible

specification in more detail (e.g. presentation, invoice, act, memo, ordinance, letter); 8) relation – determination of the direct link to another document and the type of this connection; 9) recipient – the entity to whom the document is addressed; 10) grouping – indication of affiliation to a set of documents; 11) classification – archival category of the document;12) language – code of natural language according to the ISO-639-2 standard or other language specification, if not present in the standard; 13) description – a summary, table of contents or short description of the content of the document; 14) rights – indication of the entity authorised to dispose of the document.

The Minister competent for informatization is responsible for the functioning of the electronic system, which:1) provides support for the public electronic identification system, in which the following are issued: a) trusted profile, b) personal profile; 2) enables public entities: a) to authenticate an individual using an electronic identification means, b) to ensure that an individual can sign an electronic document with a trusted signature. This responsibility is based on Article 20aa of the Informatization Act. The person applying for a trusted profile confirmed in the point confirming that profile submits an application in electronic form, using the electronic form provided in the system where the trusted profile is issued. The electronic form may be an element of the electronic service provided in ePUAP that enables the creation of an account in this electronic system – § 3 of the Ordinance of the Minister of Digital Affairs of 29 June 2020 on the trusted profile and trusted signature (Journal of Laws of 2020, item 1194 as amended).

The Minister responsible for informatization, pursuant to Article 20h of the Informatization Act, maintains a register of contact details of natural persons, designed to facilitate contact with natural persons in connection with the services and public tasks performed for these persons. The contact details are not used to contact natural persons with regard to their business activity. The register of contact details is kept in a way that : 1) allows natural persons to effectively enter, search, update and delete their contact details; 2) allows relevant entities: a) to effective enter, search, update and delete contact details in accordance with the request of the data subject, b) to search for contact details of natural persons for the purposes of provision by these entities of services and public tasks for these persons, or confirmation of the fact that no such data has been provided by the natural person searched for; 3) allows access to it 24 hours a day, 7 days a week, except for breaks for maintenance work carried out in the electronic system; 4) allows entering contact details into the register of contact data directly, in real time - § 3 of the Ordinance of the Minister of Digital Affairs of 19 December 2019 on the register of contact details (Journal of Laws of 2019, item 2467).

The Minister responsible for informatization is obliged by Article 20p of the Informatization Act to ensure the functioning of an organisational and technical solution for carrying out analyses supporting the development of key public policies using data made available by public entities, collected in public registers and ICT systems (an integrated analytical platform). In order to ensure the functioning of the integrated

analytical platform (pursuant to Article 20s of the Informatization Act), the Minister: 1) provides protection against unauthorised access to data; 2) prevents damage to the integrated analytical platform; 3) ensures the integrity of the data collected; 4) determines the rules on the security of the data processed, including personal data; 5) ensures accountability of the activities carried out under the integrated analytical platform; 6) determines the rules for reporting personal data breaches. Personal data processed under the integrated analytical platform shall be used in an adequate, appropriate and limited manner, only where necessary to achieve the specific analytical objectives. The use of data for purposes other than statutorily defined, in particular for making decisions or individual rulings, shall be prohibited. The integrated analytical platform is not intended for conducting current policy but for supporting public policies. The use of data within this platform must comply with the principle of proportionality. The use of such data must therefore not be excessive and must serve strategic analytical objectives pursued through key public policies.

The Minister competent for informatization – as follows from Article 12 AED. – shall create an address for electronic service linked to the public service of registered electronic delivery at the request of a public entity submitted to the Minister and, in the case of public entities entered in the National Court Register, automatically upon receiving via the electronic system, the data transmitted in connection with the request for entry. An application for the creation of an address for electronic deliveries linked to the public service of registered electronic delivery to a public entity contains the following data: 1) the name or business name of the entity under which the entity operates, and in the case of a court enforcement officer, his name and title; 2) the REGON identification number; 3) tax identification number (NIP), if assigned, or information on its cancellation or revocation; 4) KRS number, if assigned; 5) registered office and address; 6) address for correspondence; 7) the name of the administrator of the delivery box, his/her e-mail address and PESEL number, and if not assigned, then the unique identifier assigned by the Member State of the European Union for cross-border identification.

The Minister maintains, as a public register, an electronic address database in which addresses for electronic delivery are collected, and ensures the maintenance and development of that database. Therefore, pursuant to Article 25 AED, the Minister: 1) provides protection against unauthorized access to the electronic address database; 2) ensures the integrity of data processed in the electronic address database; 3) ensures the availability of the electronic system, in which at least: a) the electronic address database is maintained, b) search services are made available in the electronic address database, c) collects information about qualified trust service providers providing qualified electronic delivery services and about their addresses for electronic delivery and their location - for data processors in the electronic address database, and prevents damage to this electronic system; 4) determines the rules of security of processed data, including personal data; 5) determines the rules for reporting personal data breaches; 6) ensures accountability of the

activities performed on the data in the electronic address database; 7) ensures the correctness of the data processed in the electronic address database.

According to Article 58 AED, the Minister competent for informatization ensures the functioning of the electronic system, in which at least: 1) the database of electronic addresses is maintained; 2) the search services are provided in the electronic address database; 3) information is collected about qualified trust service providers providing qualified electronic delivery services and about the addresses for electronic delivery maintained by them and their location; 4) the access point to the services of registered electronic delivery in cross-border traffic is made available. Together with the Minister responsible for the economy, they both ensure the functioning of the ICT systems: 1) allowing users to access the resources of delivery boxes located in the ICT system of the designated operator; 2) allowing users to access the public electronic registered delivery service and the public hybrid service; 3) through which data about the authentication of a natural person using an electronic identification means ensuring at least an average level of security are transmitted to the system of the designated operator; 4) through which other data necessary for the provision of the public electronic registered delivery service and the public hybrid service are transmitted to the system of the designated operator.

The Minister also disposes of the Broadband Fund. This fund, as provided for in Article 16a ASD, is a public special purpose fund. The Broadband Fund is intended to be spent for: 1) measures to support the development of high-speed telecommunications networks by financing or lending for the construction or conversion of such networks and the provision of telecommunication connections to the location of the end-user; 2) actions to stimulate end-user demand for broadband services by funding the purchase of telecommunication services, the purchase of multimedia devices and the organisation of training to develop digital competences or participate in that training; 3) the costs of maintaining and operating the System of Information on Access to Fixed-Line Broadband Internet Services (SIDUSIS), which is a public database operated by the Minister responsible for informatization, including information on address points; 4) the co-financing or financing of the operation of the Broadband Coordinator, which represents the municipality or district in telecommunications matters and the development and maintenance of broadband networks within the municipality or district; 5) costs related to the operation of the Broadband Fund. The resources of the Fund may constitute revenue of the Cybersecurity Fund. As is apparent from Article 2 of the Act of 2 December 2021 on special rules of remuneration for persons performing cybersecurity tasks (Journal of Laws of 2021, item 2333 as amended), the Cybersecurity Fund is to support measures to ensure the security of information systems against cyberthreats. Its resources are allocated for an IT allowance, therefore an extra pay added to the base pay and, in the case of professional officers and soldiers, for the monetary benefit granted to persons performing cybersecurity tasks. The allowance is an incentive not only for more efficient work or service in entities carrying out cybersecurity tasks (Czuryk, 2022b: 111).

8 Administrative e-procedure

According to Article 14 CAP, cases should be processed and settled in writing, recorded in a paper form or electronic form. Documents recorded in an electronic form shall bear a qualified electronic signature, a trusted signature or a personal signature, or shall bear a qualified electronic seal of the public administration body and identification of the person who put the seal in the body of the document. Cases may be handled with the use of letters generated automatically and bearing a qualified electronic seal of a public administration body. In the case of automatically generated letters, the provisions on the necessity to affix the signature of a public administration body employee to the letter do not apply. Cases may also be handled using online services provided by public administration bodies upon authentication of a party or other participant in the proceedings.

As rightly put by the Regional Administrative Court in Gorzów in the judgment of 12 April 2018, II SAB/Go 10/18 (LEX no. 2481265), it is the responsibility of the public administration body to configure electronic mail service, including anti-spam filters, and to organise the maintenance of the body's electronic mail service in such a way as to ensure trouble-free and immediate receipt of applications sent to the address indicated by it, in view of the legal admissibility of filing them also electronically. The consequences of difficulties, errors or irregularities in the design and operation by public administration bodies of official systems for communication with them cannot be passed on to the users of these systems. The risk that an application sent to it by electronic mail, addressed to the body's officially provided electronic address, will not be received or read by the body is borne by the body and not by the applicant.

The public administration body shall deliver letters to the electronic delivery address, unless the delivery is effected on an account in the information system of the body or at the premises of the body. This rule is introduced by Article 39 § 1 CAP. If it is not possible to service the letter in this way, the delivery shall be otherwise provided. The principle of official character of delivery adopted in the CAP is expressed by the body's duty of the authority to serve mail *ex officio* in the form provided for in the statutory provisions and to ensure the regularity of the operations constituting effective delivery. Under the legislation currently in force, the use of e-mail is not a legally permissible method of service unless electronic delivery is involved – as is apparent from the judgment of the Regional Administrative Court in Warsaw of 15 January 2020, VI SA/WA 1779/19 (LEX No 3019635).

As provided for in Article 63 CPA, applications in an electronic form shall be submitted to an address for electronic delivery or through an account in the information system of the public administration body concerned. Unless otherwise provided for in separate provisions, applications submitted to the e-mail address of the public administration body shall be left unprocessed. The application should contain at least an identification of the

person from whom it originates, address of that person, including where the application is submitted electronically, as well as the request and must comply with other requirements laid down in the special provisions. The e-mail address of a public administration body cannot be equated with an electronic registry inbox, as is apparent from the judgment of the Supreme Administrative Court of 28 March 2022, I OSK 1224/21 (LEX No 3341615).

9 Conclusions

Cyberspace is a place where activities are carried out in the public, private, social or economic spheres. It is used to provide various types of services and to communicate. The importance of cyberspace for both the state and society is very important, therefore both public and private institutions have an obligation to protect it. Protection against cyberthreats should be a priority of state policy as well as the duty of entities responsible for the security of ICT systems (Karpiuk, Kelemen, 2022: 71). Cyberspace is an area allowing better fulfilment of public needs. In the age of digital government, it guarantees faster communication and more public services, and allows reaching a wider audience.

The modern public administration largely relies on ICT systems and networks that must be adequately protected against cyberattacks (Karpiuk, 2022c: 70). This protection is to be provided by the relevant authorities of the State. Thus, according to Article 32a of the Act of 24 May 2002 on the Internal Security Agency and the Intelligence Agency (consolidated text Journal of Laws of 2022, item 557 as amended), to prevent and counter terrorist incidents concerning the ICT systems of public administration bodies which are important for the continuity of the operation of the State, as well as the ICT networks listed in the uniform list of facilities, installations, equipment and services forming part of critical infrastructure or data processed in these systems, and the prevention, detection and prosecution of terrorist offences in this area, the Internal Security Agency may carry out a security assessment of these ICT systems.

Chapter IV

Legal Bases for the Operation of E-government in Slovakia

ANNA VARTAŠOVÁ & DIANA TREŠČÁKOVÁ

Abstract This chapter addresses the state of the art in the sphere of e-government in the Slovak Republic and provides for the presentation and assessment of its fundamental legal regulation and its application, focusing on the most important aspects of e-government, i.e. the electronic mailboxes, electronic submissions by natural and legal persons and deliveries of official documents issued by public administration authorities. Within this, special attention is paid to selected spheres of e-government performance which are typical for the quantity in its appearance, being the general administrative proceedings, tax administration, communication with Social Insurance Company and the courts. Following the latter, the issues connected to the performance of attorneys´ tasks are deeply analysed, focusing on the use of electronic signatures, conversion of documents and elements of e-justice applicable in Slovakia. The authors conclude, that the current legal regulation has developed to a state in which most relevant public authorities´ services are already online accessible and the user comfort of its clients has raised significantly over time, nevertheless, the e-government functions are yet not used by its addressees in the amount that would be desired and expected by the state (especially speaking of individuals), while most authors agree that still low user-friendliness of the e-services provision and too complex regulation with unresolved incompatibility issues of particular public authorities´ systems are to blame.

Keywords: • Slovakia • e-government • informatization • public authority • public administration • tax administration

CORRESPONDENCE ADDRESS: Anna Vartašová, JUDr., Ph.D., Senior researcher, Pavol Jozef Šafárik University in Košice, Faculty of Law, Department of Financial Law, Tax Law and Economics, Kováčska 26, 040 75 Košice, Slovakia, ORCID: 0000-0002-1366-0134, e-mail: anna.romanova@upjs.sk. Diana Treščáková, JUDr., Ph.D., Associate Professor, Pavol Jozef Šafárik University in Košice, Faculty of Law, Department of Commercial Law, Kováčska 26, 040 75 Košice, Slovakia, ORCID: 0000-0002-3330-1745, e-mail: diana.trescakova@upjs.sk.

https://doi.org/10.4335/2026.1.4 ISBN 978-961-7124-29-3 (PDF)
Available online at http://www.lex-localis.press.

1 Introduction

With the arrival of the electronic age, the communication of subjects of legal relations, receivers and service providers in relation to public administration, courts and other organizations is gradually changing. For this reason, it is necessary to introduce electronic systems that can mediate this communication virtually.

The electronicization of public administration is closely related to the computerization of a society. In this regard, the term "information society" comes to the fore. It can be stated that it is a society based on the penetration of information and communication technologies, information and knowledge into all areas of social life to such an extent that they fundamentally change social relations and processes.

If we talk about a definition of the term e-government, it can be stated that in the literal translation, it is electronic government, electronic public administration, or electronicization of public administration. It is an electronic interaction in which the public administration participates and in which information and communication technologies are used. We can also define e-government as the use of online information and communication technologies in public administration, which are associated with organizational changes and new skills. In its Action Plan – e-government – Action Plan 2011-2015 from 2011, the European Commission defined e-government as "the use of tools and systems that are available thanks to information and communication technologies to provide better public services to citizens and businesses".

Later in 2016, the Action Plan of the European Commission for e-Government was adopted for the years 2016-2020, which pointed out that the results of the evaluation of the previous Action Plan are positive in every direction both at the European level and at the level of the Member States. This Action Plan aimed to remove existing digital obstacles on the way to a Digital Single Market and prevent further fragmentation in the context of the modernization of public administration. The Action Plan also identified initiatives that should be based on principles that have strong stakeholder support. In the sense of the Action Plan, these principles are: 1) digital services as a standard – in the sense of this principle, public authorities should prioritize the digital provision of services. In addition, public services should be provided through a single point of contact and various channels; 2) only once is enough – public administrations should ensure that citizens and businesses provide the same information to the public administration only once; 3) inclusiveness and accessibility – public administration bodies should create digital public services that are inclusive by default and take into account different needs; 4) openness and transparency – public administration bodies should exchange information and data with each other and provide citizens and businesses with the possibility of checking and correcting their data. They should allow users to follow the administrative procedures that concern them and should involve stakeholders (such as businesses, researchers and non-profit organizations) in the design and delivery of

services and be open to cooperation with them; 5) cross-border services as a standard – public administration authorities should make relevant digital public services available across borders and prevent further fragmentation, thereby facilitating mobility within the single market; 6) interoperability as a standard – public services should be designed to work seamlessly within the single market and organizational structures, relying on the free movement of data and digital services in the European Union; 7) trustworthiness and security – individual initiatives should not be limited to the usual compliance with the legal framework for the protection of personal data and privacy, as well as IT security, but should incorporate these elements already at the design stage. These are important prerequisites for increasing trust in digital services and their implementation.

Digitization of public services is also a priority of current initiatives of the European Commission. It is one of the four basic points to be focused on by 2030. This was set out in the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions under the title - Digital Compass to 2030: A Digital Decade the European Way. By 2030, the EU aims to ensure that democratic life and public services online are fully accessible to all, including people with disabilities, and benefit from a cutting-edge digital environment that provides easy-to-use, efficient and personalized services and tools with high standards of security and privacy protection. User-friendly services will enable citizens of all ages and businesses of all sizes to more effectively influence the direction and outcomes of public administration activities, as well as improve public services. As part of a new way of building digital public services, public administration as a platform will provide holistic and easy access to public services through a seamless interplay of advanced features such as data processing, artificial intelligence and virtual reality. It will also contribute to stimulating the productivity growth of European businesses, thanks to more efficient services that are digital by default.

In general, it can be stated that the goal of e-government is to improve public administration services and the application of democratic procedures, as well as to strengthen the support of public policies. e-government includes many activities and entities (Treščáková, 2021: 122). One of the purposes is also the use of data sharing, thereby increasing the comfort of citizens and business entities when dealing with authorities and limiting unnecessary bureaucracy caused by the repeated submission of the same data to different authorities that require them. At the same time, the need to submit documents in paper form will be reduced, since the competent authority of public administration will be able to obtain it from its existing registers and possibly other information systems maintained by other public authorities. Besides providing its user with more comfort in general (Mates, Smejkal, 2012), e-government is also often connected to ensuring greater openness of public administration in relation to citizens, entrepreneurs and other entities (Macková et al., 2008). Better, cheaper[1], more reliable and more efficient provision of public administration services, optimization of existing administrative processes, accessibility and simplification of communication with public

administration for all citizens and business entities can also be identified as important goals.

The basic principles on which e-government should function are the following: 1) services to citizens – providing services by public administration bodies should be aimed at citizens and not directed against them; 2) efficiency – services provided by electronic communication channels should be offered more efficiently than conventionally provided services. In an effort to adapt to these requirements, the public administration must revaluate existing administrative processes; 3) security – electronic communication is implemented on the basis of a security policy, which is subject to the rules and practices resulting from the performed risk analysis; 4) transparency – involvement of all interested entities in the process of planning and implementation of electronic services; 5) accessibility – ensuring accessibility for everyone, i.e. for the widest possible range of users, including disadvantaged groups; 6) privacy protection – ensuring unambiguous protection of personal data and privacy; 7) multi-level cooperation – ensuring mutual communication capability for all relevant systems based on the European interoperability framework, as well as internationally freely available standards and solutions; 8) the use of "open standards", which is the international designation for freely available standards as a means of achieving interoperability; 9) technological and software neutrality – solutions must be accessible to new technologies and neutral to the specific technology used, which may favour or disadvantage a particular solution or service provider. (eGov.sk, 2008)

With regard to the various services provided by public administration, four main areas of activities can be recognized within the framework of e-government, which can also be provided in electronic form – often designated as e-government forms (Sopúchová, 2021: 47): 1) providing information to citizens via the Internet; 2) mutual communication between the administrative bodies and citizens or entrepreneurs and between the offices; 3) performance of monetary transactions; 4) e-governance – public administration (this is the extension of e-government principles to the population, by which they can participate in public administration through the use of information and communication technologies.

It can be assessed that the communication of subjects with the public administration takes place within different categories. It can be performed between citizens and public administration, business entities and public administration, public administration employees with each other, etc. Based on this, there are different levels of e-government performance defined in literature, namely: G2G – government to governments, as relations between public administration institutions; G2E – government to employees, where it is about internal relations between the public administration and its employees in the form of their online communication, G2B – government to business, as online communication between the public administration and the business environment, G2C – government to citizens, as the relations between the public administration and citizens, for example in the form of online communication, but rather from the public

administration side and C2G – citizens to government – online communication of citizens to public administration, which contrary to the previous form, it will be more about online communication initiated by citizens in relation to public administration. (Jeong, 2007; Romanová, Červená, 2016: 866, compare: Ministry of Finance, 2008: 17).

If we speak about the advantages of e-government, we can state the following advantages in particular: increasing the quality of public administration services; facilitating, speeding up and streamlining services; creation of new public services; increasing the level of awareness of the entire society; saving costs and time by the state as well as for citizens; increasing transparency and increasing citizens' trust in public administration; continuous availability of electronic services 24 hours a day, 365 days a year; increase in economic growth, reducing unemployment by improving the flow of information about job vacancies and retraining opportunities. As for the disadvantages, we could mention: the security risks of data transmission; a higher possibility of losing electronic documents, in the event of a malfunction, compared to the paper form; lack of internet connection for some areas (municipalities, businesses, households); insufficient computer skills, especially among the older generation of citizens; increase in the need for more qualified workforce in public administration institutions, increased training costs (disadvantage especially for the older generation of public administration employees); incompatibility of systems at the national or transnational level, impersonality – absence of personal contact; and the risk of data capture by unauthorized persons (Madleňáková, Madelňák, 2012: 59; Andraško, 2019: 52).

2 Legislative framework of e-government in Slovakia

As already stated, the area of e-government is part of the creation and functioning of the Digital Single Market within the EU area. Also for this reason, the legal regulation of e-government within individual member states is introduced uniformly as a whole acting "from above". We mean legislation created at the EU level, which is subsequently implemented into national legislation. The Slovak Republic is no exception.

As part of the formation of e-government, we need to base the Slovak regulation predominantly on the following EU legal acts: Regulation of the European Parliament and of the Council No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation, which repealed Directive No. 1999/93/EC); Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework, (eIDAS 2), General Regulation of the European Parliament and the Council No. 2016/679 on the protection of natural persons in the processing of personal data and on the free movement of such data (GDPR); Directive of the European Parliament and the Council No. 2006/123/EC on services in the internal market and Directive of the European Parliament and of the Council No 2014/24/EU on public procurement.

As part of the legislative activity in the Slovak Republic, the following regulations are especially important: Act No. 305/2013 Coll. on the electronic form of exercise of the powers of public authorities (e-Government Act); Decree of the Office of the Government of the Slovak Republic No. 438/2019 Coll. which implements some provisions of the e-Government Act; Act No. 211/2000 Coll. on free access to information; Act No. 272/2016 Coll. on trusted services for electronic transactions in the internal market; Decree of the Ministry of Finance of the Slovak Republic No. 331/2018 Coll. on guaranteed conversion (as amended by Decree No. 177/2020 Coll.; Act No. 18/2018 Coll. on the protection of personal data; Act No. 452/2021 Coll. on electronic communications; Act No. 95/2019 Coll. on information technologies in public administration; Act No. 343/2015 Coll. on public procurement; Act No. 315/2016 Coll. on the register of public sector partners; Act No. 530/2003 Coll. on the commercial register; Act 563/2009 Coll. on tax administration (Code of Tax Procedure) and on amendments to certain regulations; Act No. 575/2001 Coll. on the organization of government activities and the organization of the central state administration.

It can be stated that the basic legal regulation implementing the electronicization of public administration is incorporated in the mentioned e-Government Act and the Act on Trusted Services, the latter being adopted based on the eIDAS regulation.

Over time, many conceptual documents were adopted as well, but we may designate as the starting point in the field of society computerization the Society Computerization Policy in the Slovak Republic (approved by the Government in 2001) (Románová, Červená, 2017: 275). We might also mention the Action plan of the strategy of informatization of the society in the conditions of SR which was adopted by the Government in 2004, the Public administration informatization strategy from 2008, the National concepts of informatization of public administration from 2016 and 2021, operation programmes for integrated infrastructure and informatization of the society, the current Action plan for the digital transformation of Slovakia for 2019 – 2022 and 2030 Digital Transformation Strategy for Slovakia[2].

3 Position and competence of Ministry of Investment, Regional Development and Informatization of the Slovak Republic

Ministry of Investment, Regional Development and Informatization of the Slovak Republic (MIRRI) was established with effect from 1 July 2020, and, in line with Article 10 paragraph 1 letter e) of the Act No. 575/2001 Coll. on the organization of government activities and the organization of the central state administration as amended, it is responsible, among others, for central management of the informatization of the society and the creation of a single digital market policy, decision-making on the use of public funds in the public administration for information technologies, the central architecture of the integrated information system of the public administration and the coordination of

tasks in the field of informatization of the society. Thus, the tasks in the field of informatization, covered by the rest of the ministries (for their fields of management) before the change, were consolidated and merged under the competence of the new ministry. In this sphere, the MIRRI´s Section of informatization management prepares conceptual documents as well as legislation in the field of informatization of public administration and issues standards for information systems of public administration. It also monitors the status and evaluates the development of the society's informatization and manages the preparation of concepts for the development of public administration information systems. There are two organizations of MIRRI subordinated to it: The National Agency for Network and Electronic Services (NASES) and Slovensko IT, a.s.

NASES is a contributory organisation of MIRRI that fulfils professional tasks in the field of computerization of society – the operation and development of the government data network GOVNET and the services of the Central Public Administration Portal (CPAP) (Slovensko.sk), consulting, intermediary and training activities, support of the development and expansion of national e-government services aimed at simplification of the contact of citizens, entrepreneurs and the public sector with the public authorities, thus making the performance of public administration more efficient. Slovensko IT, a.s. was created as a state-owned joint-stock company that should have provided complex IT services, and innovative and cloud solutions to increase the quality and availability of such services for citizens, entrepreneurs and institutions. Its role, however, was not fulfilled and the company is not in liquidation.

Complex competencies of MIRRI are established by the e-Government Act. It contains the establishment and operation of the Central Contact Centre (which provides information on the electronic exercise of public authority and their related activities), management of the CPAP and coordination of its interconnection with other information systems. It further manages various common modules, like the electronic mailboxes module, central electronic filing module, electronic forms module, electronic delivery module, notification module, process integration and data integration module, long-term storage module and communication parts of the authentication module and payment module. The records of authentication means are also kept by the MIRRI. There is also a large list of particular detailed regulation that is to be established by the Generally binding legal regulation of the MIRRI, e.g. the details of the guaranteed conversion, details on the technical conditions and security principles of access to the electronic mailbox, the fee schedule for the operation of the CPAP and common modules, the uniform format of electronic messages sent through the CPAP and electronic deliveries, details on the method of fulfilling the obligations of public authorities in connection with the provision of electronic services, etc. (Article 59 of the Act). It also performs the control of fulfilment of the duties established by this Act and issues the methodical and interpretation tools for the implementation of this Act.

4 Specific issues connected to e-government

An important institute that was introduced for the purposes of e-government was electronic mailboxes. Electronic mailboxes are one of the most important means of communication between citizens and business entities with public administration bodies, state administration and courts.

Electronic mailboxes were established in Slovakia by the e-Government Act. Under Article 3 of this Act, an electronic mailbox is an electronic repository in which electronic messages and notifications are stored. The electronic mailbox enables citizens and business entities to communicate with public administration (offices, institutions, public authorities) electronically on a two-way (mutual) basis. Entrepreneurs and citizens can use the electronic mailbox when submitting various requests, but also vice versa, public authorities can deliver various decisions, announcements, calls, warnings, etc. to them in their electronic mailbox. In terms of content, the electronic mailbox serves to deliver the same messages that currently are (or in some cases were) delivered in paper form by post.

For natural persons, access to the electronic mailbox is enabled through an electronic identity card (eID), which is issued directly in their name and is used with a chip card reader connected to a computer. In the case of legal entities, a member of the legal entity's statutory body logs into the electronic mailbox using their electronic identity card.

According to Article 11 of the e-Government Act, electronic mailboxes are created for a public authority, a legal entity, a natural person, an entrepreneur, a subject of international law and an organizational unit, and it is free of charge. In line with the law, each person (natural or legal) can set up only one electronic mailbox for one legal status. If the owner of the electronic mailbox is simultaneously a person in several legal positions, an electronic mailbox is set up for each of these legal positions.

The term different from the creation of an electronic mailbox is its activation. Under Article 13 paragraph 1 letter a) of the e-Government Act, the activation of an electronic mailbox is understood as an action performed by the administrator of the electronic mailbox module, which enables the use of the electronic mailbox for electronic delivery.

Currently, electronic mailboxes are set up for all natural persons, including entrepreneurs and self-employed persons, as well as legal entities – not only entrepreneurs, i.e. commercial companies, their organizational components and cooperatives, but also other non-business legal entities (churches, political parties, foundations, etc.).

Activation of the electronic mailbox is voluntary for natural persons (except for entrepreneurs). A natural person - a citizen of the Slovak Republic does not have their mailbox automatically activated for delivery when it is created. To activate the mailbox, he must request it. If the citizen has an activated mailbox, the decisions of the public

administration bodies can be delivered to him electronically, while their legal effect is the same as if the decisions were delivered in paper form. However, if the citizen does not have an activated mailbox, decisions must be delivered to him only in paper form (Treščáková, 2021: 134).

In order to complete the entire process of the electronicization of public administration, it will be necessary for entities that have not yet had the obligation to have an activated electronic mailbox and to communicate electronically with public administration bodies, to start this process of overall electronicization (Treščáková, 2020: 30).

The e-Government Act distinguishes between the terms deactivation and cancellation of an electronic mailbox. In practice, the terms deactivation of an electronic mailbox and its cancellation are often confused, and it is necessary to distinguish between these terms.

Deactivating an electronic mailbox is an act that ensures that the electronic mailbox cannot be used further for electronic delivery, while access to it and its contents are not affected. Deactivation of the electronic mailbox does not automatically cancel it. Cancellation of an electronic mailbox is preceded by its deactivation. Deactivation of an electronic mailbox activated for delivery during the life or existence of the subject to whom it was established is not possible in any way, according to the law. The electronic mailbox of an individual will be deactivated either by death or the validity of a judgment declaring him dead, or by a valid decision on deprivation or limitation of capacity for legal acts, if this limitation also includes legal acts associated with disposal of an electronic mailbox. The legal entity's electronic mailbox will be deactivated only after it ceases to exist, i.e. removal from the commercial register.

Subsequently, the cancellation of the electronic mailbox consists in preventing access to it, as well as deleting its contents. According to the e-Government Act, an electronic mailbox will be cancelled after three years from the day when the administrator of the electronic mailbox module learns about the death of its owner, the declaration of its owner as dead or the deletion of its owner without a legal successor.

The concepts of electronic submission and electronic delivery are closely related to the electronic performance of public administration and electronic mailboxes. Electronic submissions are subsequently followed by an electronic signature and the related electronic identity.

Electronic submission is regulated in Article 3 letter j) and Article 24 et seq. of the e-Government Act. Electronic filing means data filled in according to an electronic form, which is sent electronically to a public authority by a person who is a party to the proceedings for the purpose of exercising public authority or initiating it.

Electronic filing, including attachments, has the same legal effects as a motion to initiate proceedings, a lawsuit, request, complaint, statement, opinion, notification or other document, including attachments, that is filed or delivered to a public authority in paper form. Electronic submission, including all electronic documents, is considered to have been delivered by depositing it in a mailbox, i.e. at the moment when the electronic official report is objectively available to the recipient in the electronic mailbox.

The public authority is obliged to receive electronically delivered electronic messages every day. For the received electronic submission or electronic document, the public authority is obliged to issue a receipt. If the addressee is a public authority, the delivery note is created and confirmed by the electronic filing office of this authority. The delivery note contains information about the day and time when electronic delivery occurred, recipient and sender identifiers, and electronic messages and electronic documents that are delivered electronically.

An important concept related to electronic filing is electronic form. In the sense of the e-Government Act, it is an electronic document containing automatically processed rules, through which it is possible to fill in and present the filled data in a structured form by electronic means.

The content requirements of the electronic form for electronic submission are the content requirements of the proposal for initiation of proceedings, lawsuits, requests, complaints, statements, opinions, announcements or other documents established by special regulations, while if any of the content requirements are bound to a written form according to special regulations, it is considered for fulfilled by authorizing the electronic submission by the submitter.

Attachments to electronic filing are always attached as a separate electronic document, while if the attachment exists only in paper form and according to a special regulation it is required to be submitted at least in an officially certified copy, it is attached to the electronic filing as an electronic document that was created by guaranteed conversion.

The attachment of attachments to the electronic filing is done by inserting the electronic filing together with the attachments into the electronic report through the dedicated function of the CPAP or a specialized portal, which will ensure the connection of the electronic filing and the attachments and the preservation of the link between them.

Electronic submission is possible by electronic forms or in line with Article 24 paragraph 8 of the e-Government Act, through a specialized portal (CPAP) available on the website https://www.slovensko.sk.

The Slovensko.sk portal is one of the most widely used public administration information systems, which is used not only by the general public but also by entities communicating

with the courts, due to the simplicity of filing submissions. As already mentioned, in the case of making submissions through this portal, it is not necessary to fill out forms, simply to "upload" the submission.

CPAP ensures central and uniform access to information resources and public administration services. Among the most important tasks of the CPAP is directing the user to use a specific public administration electronic service using relevant information sources, such as the portal of financial administration.

The content of the portal includes digital content in the form of supporting information for the use of the service and the provision of electronic services itself. The concept of the CPAP content is governed by the following principles: Firstly, organization of information and services according to spheres of life situations – services on CPAP are logically divided according to the target group (citizen/entrepreneur/institution) and spheres of life situations, which make available information and services arranged in alphabetical order. This concept makes it possible to access the required information resources as well as electronic services in a structured manner, according to the user's actual requirements, and to filter the extensive content of the CPAP in a targeted manner. Secondly, virtual centralization - from the point of view of the users of the CPAP services, the portal represents a centralized solution where all information is available from one place and logically structured electronic services are accessible in a unified way.

An important area related to the electronic performance of public administration, without which the purpose of e-government would not be fulfilled, is the application of law in individual cases (i.e. decision-making activities of public authorities) in an electronic way, especially through electronic mailboxes. As already mentioned above, public authorities and courts now communicate automatically through electronic mailboxes basically with legal entities, as well as with natural persons who are entrepreneurs and those who have voluntarily activated their electronic mailboxes. Communication is two-way. Electronic legal acts can include electronic delivery, electronic filing, simple or guaranteed conversion of documents, etc.

Electronic delivery is regulated in Article 29 et seq. of the e-Government Act. Electronic submissions and electronic official documents are delivered electronically, while the place for electronic delivery is an electronic mailbox that is activated. The main function of the established and activated electronic mailbox is to receive official electronic messages from public administration bodies. It should be noted that the electronic mailbox does not fulfil the function of communication on a private basis, or between business entities or natural persons with each other. Electronic mailboxes were established for communication with public administration bodies, as well as with judicial authorities.

As for delivery itself, even in the case of delivery of electronic messages to electronic mailboxes, a distinction is made between messages delivered to one's own hands or not (Lechner, 2013: 44). In the case of delivery of messages to the subject's own hands, the recipient is obliged to confirm the so-called electronic delivery note and only after that, the content of the message will be made available to him. The relevant authority, as the sender of this message, is also informed by the notification about the confirmation of the electronic delivery note and thus the reading of the message. In the case of confirmation of the electronic delivery note, it will be considered that the message was read immediately after it was made available. However, if the subject does not confirm the electronic receipt, after the expiry of fifteen days from the day following its receipt in the electronic mailbox, the message will be considered read, regardless of whether the subject has actually read it or not. So the fiction of delivery applies. Electronic documents delivered electronically to one's own hands are, in terms of legal effects, identical to a document in paper form delivered to one's own hands in accordance with special regulations (e.g. Civil Dispute Procedure).

The electronic delivery note is an electronic document containing information on the day, hour, minute and second of electronic delivery, the recipient's personal identifier, the sender's personal identifier and the identification of the electronic official report and electronic documents that are delivered electronically. The moment when an electronic message is considered delivered is also important. Following Article 32 paragraph 5, the electronic official report (including all electronic documents) is considered delivered: (a) if the addressee is a public authority, by depositing an electronic official report; (b) if the addressee is not a public authority and it is delivered to its own hands, on the day, hour, minute and second indicated on the electronic delivery note or by the expiration, in vain, of the storage period, whichever occurs first, even if the addressee did not learn about the message (the fiction of delivery applies here as in court proceedings) or (c) if the addressee is not a public authority and it is not delivered in own´s hands, the day immediately following the filing of the electronic official report.

If the electronic delivery takes place on a public holiday or a non-working day, the time limit for action or the performance of an act, the beginning of which is connected with the moment of electronic delivery, will begin on the next working day, unless it is stipulated by a special regulation that the public authority or another person also works on a day that is a national holiday or a day of rest. In connection with the moment of delivery, there are problems in application practice regarding the assessment of when the submission was actually delivered. The resolution of this issue is particularly important from the point of view of compliance with the deadlines that are established by law for certain procedural actions. It is necessary to refer to case law in this regard. For example, the Supreme Court of the Slovak Republic in its decision of 25 June 2019, case No. 5 Cdo 75/2019 comments on the deadline for submitting an appeal electronically, stating that to maintain the deadline for filing an appeal, the moment of sending the electronic submission will be decisive in the given case according to the last sentence of Article 25

paragraph 1 of the e-Government Act without the need for further proof of the actual delivery of the submission from this system to the designated court. This also fully corresponds with the wording of Article 121 paragraph. 5 of the Civil Dispute Procedure Code regarding the preservation of procedural deadlines. The party to the dispute cannot be burdened with the process of subsequent transfer of data from the portal to the designated court, as it cannot influence this stage of delivery. The finding of the Constitutional Court of the SR, case No. III. ÚS 479/2018 implies that the notification containing the date of the successful submission of the electronic submission to the system must be considered as evidence determining the assessment of compliance with the deadline for making the submission established by law or determined by the court, i.e. also as evidence determining the timeliness of filing a remedy.

Closely related to electronic mailboxes, electronic delivery and filing is the issue of digital identity. It can be stated that all entities that use electronic means, whether in the employment, business or private sphere, have their own virtual identity. Virtual identity, or identification of the person making an electronic legal act is more than necessary. Legal acts in the virtual world are carried out towards absent persons, and that is why there is an increased emphasis on determining (proving) the identity of the person making the legal act, both in the case of natural and legal persons (Frimmel, 2002: 324).

e-Government Act in its Article 3 defines the "identification" as declaring the identity of an object, including a person, especially when accessing the public administration information system or during electronic communication. Authentication in this legal regulation means proving the identity of an identified object, usually through an authenticator. In the sense of the provisions of Article 19 paragraph 1 of the e-Government Act, a person's electronic identity is a set of attributes that can be recorded in electronic form and that clearly distinguish one person from another, especially to access the information system or for electronic communication. A person's electronic identity is declared by person identification and verified by person authentication.

It is generally known that when performing legal acts in a normal environment, without the use of electronic means, a natural person identifies himself by his first and last name, date of birth and birth number. For these purposes, a national identity card is normally used, or another document confirming the identity of the person in question (for example, proof of health insurance, driver's license, etc.). The identifier of a natural person in the case of electronic communication within the meaning of the e-Government Act is his birth number in combination with his first and last name. The identifier of the public authority is the identification number of the organization, and if the public authority is not assigned one, the identifier is a set of characters assigned according to a special regulation.

Currently, an electronic identity card or electronic identification card (eID), which is an ID card with an electronic contact chip, serves to prove a person´s virtual identity. The mentioned question is closely related to electronic mailboxes, which cannot be used

without an eID. Citizen cards with an electronic contact chip began to be issued on 2 December 2013 as part of the process of electronic public administration, in which public administration services were made available to citizens via the Internet through e-government services.

The identification data of the citizen that are stored on the ID card chip, are namely the name, surname, residential address, date of birth, as well as data on the validity of the ID. In addition, certificates for the creation of a qualified electronic signature can be stored on the chip, based on which it will be possible to create a qualified electronic signature, as well as certificates necessary for encryption of communication with the ID card, or other data. The electronic chip fundamentally expands the possibilities of using the identity card. In the case of an identification document without an electronic chip, personal contact is required when proving the holder's identity with public or commercial institutions. The ID card with an electronic chip extends this use to electronic communication via the Internet.

5 Electronic communication in assorted areas of public administration

From the viewpoint of common natural and legal persons, we consider as decisive the ability to communicate with government bodies by electronic means, including the possibilities for electronic submitting and delivering official documents. Currently, from the point of view of de lege lata status, within the framework of the electronicization of public administration, private entities have the opportunity to use electronic services in several areas of fulfilling obligations or exercising rights in relation to public authorities, and that, one might say, of the most relevant ones. Through the CPAP, a complex set of public authorities, which have a certain range of their electronically available services registered and accessible directly on this portal, is accessible to the public. Among these, there are such authorities and entities as particular ministries, the Office of the Government of the Slovak Republic, the Office of Geodesy, Cartography and Cadastre of the Slovak Republic, the Office of Industrial Property, the Slovak Trade Inspection, the Office for Public Procurement, the Office for the Regulation of Network Industries, the Supreme Audit Office of the Slovak Republic, the Antimonopoly Office of the Slovak Republic, health insurance companies, municipalities, cities and self-governing regions, bailiffs, notaries and the Chamber of Notaries of the Slovak Republic, courts, prosecutor's offices, Social Insurance company, labour, social affairs and family offices, district offices, Financial Directorate, tax and customs offices and other public authorities, schools, and other institutions. A motivating factor supporting the use of electronically available public administration services is also the reduction of fees for electronic submissions to half the standard rate of administrative and court fees, which was introduced in December 2013 (Románová, Červená, 2016: 869); this benefit is now more limited.

The basic act regulating general administrative proceedings, i.e. Act No. 71/1967 Coll. on administrative procedure (Code of Administrative Procedure), as amended, provides in Article 19 that filings can also be made by electronic means, but shall be signed with a guaranteed electronic signature according to a special law, i.e. the e-Government Act and shall contain the identifier of the person involved in the proceedings according to this Act. A filing in the main matter made in electronic form lacking the authorization according to the e-Government Act shall be completed within three working days in paper form, properly authorized in electronic form, or orally in the minutes, while the administrative body does not call for further additions of the filing.

The Code of Administrative Procedure also provides for the issuance of documents by administrative authorities in electronic form and for this purpose stipulates that the decision in electronic form does not contain an official stamp and signature, but is authorized by the administrative authority following the e-Government Act.

In the area of taxes, Act No. 563/2009 Coll. on tax administration (Code of Tax Procedure) and on amendments to certain regulations as amended regulates the two-way electronic communication between financial authorities and tax subjects, namely the filings addressed to financial administration authorities and the delivery of documents issued by these authorities addressed to tax subjects. In both cases, the regulation is governed by the Code of Tax Procedure, unless the e-Government Act as lex specialis provides otherwise in the provisions on electronic filing and delivery. Electronic filing and delivery were supposed to be prioritised right from the beginning of this Code´s applicability (Románová, Červená, 2015: 330), however, the practical application kept lagging behind the theoretical legal regulation (Románová, Červená, 2016: 870), mainly due to the repeated postponement of the effectiveness of introduced changes in the level of electronicization (Kačaljak, 2017: 46), which occurred as a result of technical unpreparedness for the implementation of the already approved legislation and practical application problems (Románová, Červená, 2015: 331).

As regards the tax subjects' electronic filings, this is carried out through a specialized Financial Administration, portal operated by the Financial Directorate of the Slovak Republic, (or through the electronic filing office of the CPAP, which redirects the client to this portal). Such electronic filing can be implemented in two ways. The first is a filing authorized by a qualified electronic signature, and the second is the so-called "another recognized way of authorization" according to the e-Government Act, i.e. based on a written agreement on electronic filing concluded between the tax subject and financial administration authority. This second method is only accessible to natural persons who cannot/do not want to use authorization through a qualified electronic signature. Such a person shall notify the tax administration authority of the data required for delivery of filing (in a structured form as published on the website of the Financial Directorate) and conclude the above-mentioned agreement with the tax administration authority, which includes, in particular, the details of electronic delivery, the method of verifying

electronic filing and the method of proving delivery. An electronic filing submitted in any other way (e.g. by e-mail) shall also be delivered in paper form or electronic form in one of the two ways indicated above (signed with a qualified electronic signature or following the agreement on electronic filing) within five working days from the day of filing, otherwise, it is considered undelivered. On a theoretical level, we can therefore distinguish between "qualified" electronic filings and "unqualified" electronic filings (that is, requiring supplementation – sending in a qualified form).

Electronic filing is available to entrepreneurs and wide public, as well, and may be used as a time-consuming way of submitting. In principle, the choice of the method of submitting the filing (whether in person, in writing or electronically) is up to tax subjects, however, the Code defines a group of them for which the obligation to make filing only electronically (in a qualified manner) is set in its Article 14 since 2014: Firstly, it is the tax subjects who are the VAT payers; secondly, tax advisors for the tax subjects whom they represent in tax administration; thirdly, lawyers for the tax subjects whom they represent in tax administration and fourthly, other representatives for the tax subjects mentioned in the first case whom they represent in tax administration. This has been enlarged to legal entities registered in the commercial register and natural persons-entrepreneurs registered for income tax and their representatives since 2018. In this way, they are required to make not only filings whose forms are included in the catalogue of electronic forms, such as tax returns, but also other filings, such as applications, notices, appeals, initiatives, complaints, statements, objections, responses to calls from tax administrators, etc.[3] (Romanová, Červená, 2016: 870). Since 2016, the regulation has been supplemented that if they do not submit their filing electronically, they will be invited by the tax administrator to do so. The reason was that the beginnings of this compulsory electronic form of filing were connected with many practical problems[4] and confusion, especially on the side of taxpayers and their representatives[5] , but also tax administrators who were unsure what should be the result of failing the duty and often refused to accept the filing, which caused the lapse of periods to the detriment of taxpayers[6] . It was also set by the case law in this regard, that a purely electronic way of filing cannot be requested from these entities in case of filing an appeal, since its special regulation of Article 72 paragraph 1 explicitly enables doing so in written and oral form; when interpreting the provisions of Article 14 paragraph 1 letter a) of the Code, the grammatical interpretation cannot be accepted, because it would be contrary to the principles of the tax procedure itself, but above all to the principle of legality and the principle of the right to judicial protection[7] .

If the filing is a tax return, due to the so-called stricter written form (that is, the necessity to submit a filing using the prescribed form), which remains even with electronic filing, it is necessary to submit the return in the prescribed form, i.e. using the relevant electronic form. Since 2016, it was amended that failing to file such document in an electronic form shall be treated as undelivered filing, however, since 2020, this amendment was repelled due to its harshness and the solution to such failure was put in line with the regulation of

general filing duties of these subjects, i.e. that failing to file electronically will lead to act of tax administrator inviting them to do so.

The Code also provides for cases where the submission in electronic form cannot be delivered for reasons on the part of the tax administration authority; then the deadline is considered to be preserved if the filing is delivered on the next working day after the removal of obstacles on the part of the tax administration. This technical factor, especially in the past[8], often failed, which resulted in frequent encounters with such a situation and, subsequently, comprehensive hereto associated disputes between the taxpayers and tax administration. The solution that was adopted is the guideline on using the remedy of request for remission of default of time limit (within 30 days after the date when the reasons for the default disappeared and if the taxable entity makes the defaulted action within the same time limit) according to Article 29 of the Code.

The second counterpart is the delivery of documents issued by the tax administrator and the Financial directorate to tax subjects. According to the Code of Tax Procedure, these are primarily delivered by electronic means[9], while other forms should be used only if this is not possible. According to the e-Government Act, the place for electronic delivery is an electronic mailbox, if activated. All documents that, according to the Code of Tax Procedure, are to be delivered into own hands are delivered electronically in a mode that requires confirmation of delivery by the addressee or a person to whom, according to special regulations, it is possible to deliver instead of the addressee (e.g. a representative), in the form of an electronic delivery note sent to the sender. The full application of this electronic delivery (in regards to all the taxes and subjects that have activated their electronic mailboxes at Slovensko.sk) was only started in 2022 and the communication was transferred from the separate portal of financial administration to the CPAP (Slovensko.sk). Before this, the delivery in customs duties started only in 2016. As mentioned above, technical problems have been accompanying the delivery, as well. For this reason, in case of technical errors in the delivery of tax administration´s documents, the process of a motion for the ineffectiveness of delivery[10] is governed by Article 33 of the e-Government Act. This institute and remission of default of time limit may not be interchanged, since the decision on ineffectiveness of delivery only enables the party to get acquainted with the "undelivered" decision and make filing (in time) on its basis (Andraško et al., 2019, p. 58 following the Resolution of the Constitutional Court of the Slovak Republic in case No. I. ÚS 101/2019-13). Here it is important to mention that if the public authority has decided that electronic delivery is ineffective, the electronic official message, including all electronic documents, is considered delivered on the day when the decision on the ineffectiveness of electronic delivery became final. For this reason, ex officio deciding on ineffectiveness is not allowed in case that a special regulation does not make it possible to exclude the effects of substitute delivery, such as in case of delivery of tax enforcement notice according to Article 91 paragraph 3 (shall only be delivered into own hands).

However, in addition to these two basic elements of electronic communication, the tax administration also offers more complex electronic services in the form of a tax subject's personal Internet zone, to which the tax subject will have access through the Financial Administration portal (accessible either through an identifier and password or through the Slovensko.sk portal). The contents of the personal internet zone are mainly the file of the tax subject in electronic form, an electronic statement from the personal account of the tax subject, access to the electronic filing service, an electronic personal mailbox and a catalogue of services.

The provision of electronic services is also enabled (and anticipated) by Act No. 582/2004 Coll. on local taxes and the local fee for municipal waste and small construction waste, as amended, which, in general, was in the beginning associated with many complications connected to the overall situation of especially smaller municipalities as regards their technical ICT and personnel equipment (Románová, Červená, 2017). A significant change in legal regulation took place from 1 November 2023. The original regulation stipulated only the authorization of the municipality for voluntary provision of electronic services, in the form of authorized access by the taxpayer to the taxpayer's personal Internet zone after entering access data on the website of the municipality, which contained a similar framework as in case of state taxes. Such services as well as details regarding their provision had to be established by the municipality in a generally binding regulation published on its website (Románová, Červená, 2016: 871); this regulation remains preserved. However, according to the new regulation, municipalities will be allowed (in a formally regulated manner) to partially communicate electronically even with a tax subject who does not have an activated electronic mailbox, and for the tax period of 2024, with their consent, municipalities will be allowed to send them a notification about the amount of the tax/fee and the deadline for its payment to their email address or via their personal Internet zone. If the tax subject pays it, it is considered to have been levied on the day of payment, and if not, its non-payment is not considered an administrative offence and therefore no fine is imposed for it at this stage, hence, the municipality will levy the tax/fee in the form of a standard decision, which will be delivered in the usual way. Whether the municipality will proceed in this way and the details of such procedure will be regulated by the municipality in a generally binding regulation. Such an opportunity will help reduce the administrative burden of municipalities within the administration of local taxes.

Following the new legislation, the municipality shall also, from the tax period of 2025, provide the service of a pre-filled real estate tax return to the tax subjects using the electronic service of the real estate cadastre when submitting a proposal for the initiation of cadastral proceedings, if the electronic service of the municipality is integrated into the information system of the central administration of reference data. The new regulation also stipulated that the municipality no longer has to make the taxpayer's personal Internet zone available on its website, but can also use the information system of the Data Centre of Municipalities and Towns (DCOM) for this purpose. DCOM is a supra-departmental

information system for self-government embedded in the e-Government Act, which was of the end of 2023 used by approximately 70% of municipalities and cities. Its preparation started in 2011 and it was implemented with the specific aim of supporting (especially smaller) municipalities and cities, that might have struggled with the preparation of functioning within the electronicization of public administration and particularly, providing their services electronically (Románová, Červená, 2017). It offers not only electronic services but also ten integrations with other public administration registers and databases, as well as a link to the original information system of local governments, thanks to which it includes the entire agenda resulting from the original competencies of local governments. It also includes, for example, intelligent forms that limit the need to manually enter a lot of data, which simplifies and speeds up the work of office employees (www.dcom.sk, 2023)[11]. The project also includes the mID mobile application, which enables individuals and legal entities to use the online services of municipalities, in a range depending on whether a specific municipality uses the DCOM information system or not - if the municipality is connected to the system, over 130 online services are directly accessible from a mobile phone, and if it is not, the possibility to use at least the so-called general submission service is currently in preparation (www.vybavzmobilu.sk, 2023).

Under Act No. 461/2003 Coll. on social insurance as amended (Social Insurance Act), Social Insurance Company provides for electronic communication with its clients. In the same way as the Code of Tax Procedure, the Social Insurance Act also focuses attention on the electronicization of communication between obliged entities and the Social Insurance Company, while similarly enshrining a dual mode of communication by electronic means, either with the use of a guaranteed electronic signature or in another way (without the need to have a qualified electronic signature) based on of the written agreement concluded with the Social Insurance Company for these purposes, which according to Article 186 paragraph 2 will contain, in particular, the requirements of electronic delivery, the method of verifying the submission made by electronic means and the method of proving the delivery of the document. However, unlike the area of taxation, the Social Insurance Act does not enshrine electronic delivery as a priority, only as one of the available forms. The insurance company uses its own specialised portal for this purpose. It comprises complex e-services for employers and self-employed persons who are insurance premium payers, health care providers, institutions, and other departments, the electronic account of the insured persons and the access to e-forms.

6 Performance of attorneys´ tasks

With the arrival of the electronic age and the introduction of electronic systems into every area of our operation, communication between public administration bodies, courts and business entities was also introduced. Business entities also include lawyers, whether they provide legal services as individuals, i.e. natural persons – entrepreneurs or as groups of lawyers, e.g. companies. Attorneys are obliged to communicate with the courts electronically. If the entity, whether it is a natural person or a legal entity, is represented

by an attorney, it is not possible to communicate with the court outside the online sphere. Of course, participation in hearings is personal. However, there are exceptions when the participation of a party to the proceedings or, for example, a witness can be connected online and the witness will be interviewed via a video call. Filing actions, statements, etc. is carried out exclusively electronically. If the person is not represented by an attorney and does not have an activated electronic mailbox for electronic delivery, he can communicate with the courts personally in such a case.

Attorneys have an automatically set up an electronic mailbox and are required to have it activated for electronic delivery. Access to the electronic mailbox is performed via an electronic identity card. If the lawyer is an individual, he logs in via his eID. In the case of a commercial company, a statutory body, e.g. managing director, is logged into the electronic mailbox. With the electronic ID, it is possible to download electronic documents from the electronic mailbox and read the messages, but to make electronic submissions, it is, in addition, necessary to have an electronic attorney's card equipped with an electronic chip. The certificates necessary for the authorization of electronic filing and thus for electronic signing are recorded on the electronic chip.

In this context, it is necessary to refer to the decision of the Constitutional Court of the Slovak Republic, case No. I. ÚS 484/2019, in the light of which, in view of the fact that pursuant to Article 82l of Act No. 757/2004 Coll. on Courts and Amendments to Certain Acts, as amended, lawyers (legal entities from 1 July 2017 and natural persons from 1 July 2018) are obliged to deliver submissions to the court's electronic mailbox and to use within the electronic communication with the court in proceedings the electronic mailboxes activated for delivery, of which they are the owners, the mandatory requirement of the summons according to the second sentence of Article 429 paragraph 1 of the Code of Civil Procedure consisting in writing the appeal by an attorney, will be considered as fulfilled if the appeal is submitted electronically and authorized by a qualified electronic signature or a qualified electronic seal belonging to the attorney who represents the appellant. It is basically without legal significance to investigate which natural person created the written document, or how many natural persons participated in its creation. Among other things, it is a matter of the proper attorneys´ practice that the electronically filed appeal of the client whom the attorney represents is authorized by a qualified electronic signature or a qualified electronic seal belonging to the attorney (Article 23 paragraph 1 of the e-Government Act). If he does not do so and, as a result, an act resulting in a negative consequence concerning his client's case is thwarted, this may establish his disciplinary responsibility and the possibility of the client claiming compensation for damages caused in connection with the attorneys´ practice.

The electronic signature is regulated in Section 4 of Article 25 – 34 of the eIDAS regulation and in Slovak legal conditions it is regulated by Act on Trusted Services. The regulation emphasizes the recognition of electronic signatures both in court and in administrative proceedings so that they are not denied legal effects and are not rejected

as evidence. It follows from the above that an electronic signature should have the same legal effects as a "classic" signature contained on a document in paper form (Smejkal, Kodl, Uřiča, 2015: 190).

With the help of a qualified electronic signature, it is possible to carry out legal acts electronically, which in the "paper world" requires a written form, i.e. in this case, a qualified electronic signature replaces the written form of a handwritten signature. The above is also based on the provisions of Article 40 paragraph 4 of the Civil Code, which states that "the written form is preserved if the legal act is made by telegraph, teletype or electronic means that allow the content of the legal act to be captured and the person who made the legal act to be determined." The written form is preserved whenever a legal act made by electronic means "is signed with a guaranteed electronic signature or a guaranteed electronic seal." The Civil Code in this case uses the terms guaranteed electronic signature and guaranteed electronic seal. In the sense of the provisions of Article 17 paragraph 2 of the Act on Trusted Services, the term guaranteed electronic signature is used in generally binding legal regulations, meaning a qualified electronic signature. When the term guaranteed electronic seal is used in this legislation, it means a qualified electronic seal, and when the term time stamp is used, it means a qualified time stamp.

It should be emphasized that only a qualified electronic signature is given the same status by the eIDAS regulation as a handwritten signature, and such a signature must be in the sense of Article 25 of the regulation recognized by all member states. A qualified electronic signature is an improved electronic signature created using a qualified device for creating an electronic signature and based on a qualified certificate for electronic signatures. This is a signature with the highest credibility. The signature created by the certificate has the same legal effect as a handwritten signature, and a token or chip card, where the keys are stored, must be used for making the signature. Such equipment is called a qualified means for creating electronic signatures.

If a qualified electronic signature is used to sign an electronic document, the electronic document will have the following properties: 1) authenticity – the identity of the subject who created the signature can be unequivocally verified and a qualified certificate for electronic signature has been issued to that person; 2) integrity – it can be demonstrated that after signing the document, there was no intentional or unintentional change in the content of the document, as it was at the time of its signing; 3) non-repudiation – the author cannot claim that he did not make the given signature of the electronic document.

The security of a qualified electronic signature is ensured by the use of a qualified means for creating an electronic signature. In general, it can be stated that a qualified electronic signature will be usable: 1) when communicating with public authorities through the CPAP; 2) in the form of a universal submission for various entities (notaries, executors, state administration organizations, cadastral offices, etc.); 3) when communicating with

the Commercial Register (from 1 January 2020 only electronically) and communicating with the Trade Office; 4) when communicating with the Financial Administration of the Slovak Republic; 5) when communicating with the courts.

Conversion is a procedure in which the entire information content of the original document, whether paper or electronic, normally perceptible by the senses, is transformed into a newly created electronic or paper document. Attorneys use a guaranteed conversion to preserve the legal effects of the original document and its applicability to legal acts carried out by the guaranteed conversion procedure. At the same time, the law determines the persons who are authorized to perform the guaranteed conversion. These are: 1) public authority, lawyer and notary public; 2) a postal company providing a universal service, if it is the operator of an integrated service point; 3) patent representative, if it is not a conversion of a public document; 4) The Slovak Land Fund, if it is a guaranteed conversion of documents for its own use to carry out its activities.

The purpose of the conversion is to ensure the possibility of transfer between paper and electronic forms of documents or electronic forms of documents with different formats so that the newly created document has the same legal effects and can be used for the same legal purposes as the original document. For example, a document in paper form, of which it is not possible to make an officially certified copy according to special regulations, or a document in paper form, the uniqueness of which cannot be replaced by conversion, in particular, an identity card, travel document, money, securities, etc., cannot be converted. This applies also to audio files or video files.

Attorneys use guaranteed conversion for documents that form attachments to submissions, i.e. attachments to the actions, to the statement, supporting evidence, etc. It is mainly about the conversion of paper documents that are officially certified into electronic form. A power of attorney for representation must always be converted by a guaranteed conversion (Resolution of the Constitutional Court of the Slovak Republic of 31 May 2018, case No. IV. ÚS 342/2018 - Authorization of a power of attorney by a lawyer as a proxy is not sufficient, because it only proves the authenticity of the proxy, and thus the fact that the attorney has accepted the power of attorney - it can be problematic in proceedings in which the participants must be represented by an attorney.

7 E-justice as a part of e-government

A part of the electronic performance of public administration (e-government) is the electronic performance of the judiciary (e-justice). In general, e-justice means the use of information technologies and systems in the judiciary environment, but primarily, it is perceived as the introduction of an electronic form of communication, exchange and processing of information among subjects operating in the judiciary environment or entering the judiciary environment from the outside, i.e. participants in the proceedings, administrative authorities, etc.). The goal of e-justice is to facilitate and streamline work

in the judiciary environment, to speed up processes and thus to speed up the completion of court proceedings (Fridrich, Paľko, 2012: 20).

The areas covered by e-justice comprise: 1) registers based on an electronic basis; 2) obtaining evidence, procurement of evidence, and presentation of evidence in courts; 3) correspondence both inside the courts and outside with the participants in the proceedings - notification of actions, sending submissions, etc.; 4) enforcement of judgments; 5) special proceedings; 6) payment orders; 7) requests for legal assistance; 8) alternative dispute resolution methods.

As regards the implementation of e-justice in Slovakia, it can be stated that the e-justice project was launched simultaneously with the launch of the e-government project in Slovakia. The first step in connection with the electronicization of the judiciary was the implementation of the Court management project, which ran from 1999 to 2005. As part of this project, the first electronic system in the judiciary was introduced, namely the information system - Registry. Its goal was to create a program and application for random allocation of the actions to senates, or the judges. In the first phase, this information system was "tested" at the District Court in Banská Bystrica, and subsequently, after its success, the second phase began and this system was installed in all district and regional courts in the Slovak Republic.

As part of the Court Management project, Act No. 185/2002 Coll. on the Judicial Council was adopted, which in Article 26 paragraph 2 established that, in accordance with the work schedule, cases are allocated to judges and higher court officials by random selection using technical tools and program tools approved by the Ministry of Justice of the Slovak Republic in such a way that the possibility of influencing the assigned cases is excluded. This provision was later reflected in Act No. 757/2004 Coll. on courts. Currently, this way of allocating cases can be found in Article 51.

In 2006, another step followed and it was aimed not only at the electronicization of the judiciary but also at the so-called open courts. Publication of court decisions in electronic form was introduced. This was also launched based on the recommendations of the Council of Europe on the publication of court decisions on the Internet. The aforementioned started to be implemented in May 2006 through JASPI – a non-commercial legal information system. It was originally launched only for state authorities, but later also for the public. Subsequently, a project under the name "Development of electronic judicial services" was implemented between 2013-2015. The goals of the project were, first of all, the electronicization of court services, which up to that time only took place in a paper form, and also the introduction of new electronic services of the judiciary and the implementation of new information systems, as well as the creation of a safe and reliable repository for all information systems of the judiciary. The creation of a video conferencing system for the judiciary was another part of it.

Subsequently, with the adoption of the e-Government Act, there was a gradual implementation of electronic communication between courts and parties in proceedings by electronic mailboxes via the Slovensko.sk portal or via the e-action portal operated by the Ministry of Justice of the Slovak Republic, which took its current form on 1 February 2017. Through this portal, actions for the initiation of proceedings are submitted via e-forms. It is up to the attorney whether he decides to submit to the courts through the Slovensko.sk portal or the e-action portal. The difference, however, is that if he submits through the e-action portal, he must complete the submission using a completed form. Through the portal Slovensko.sk, the application is submitted in the format of an electronic document, which is, for example, converted from a Word or PDF document prepared by the attorney on his computer. However, it should be noted that in the case of submissions within the so-called reminder proceedings, enforcement proceedings or the Register of Public Sector Partners, the lawyer's submission must be made only through the e-action portal, i.e. by filling in the relevant forms. Since July 2017, public authorities, attorneys, bailiffs, notaries and administrators of the bankruptcy estate are, according to the provisions of Article 82l paragraph 3 of the Act on Courts, obliged to deliver submissions to the court's electronic mailbox in proceedings before the court and use the electronic mailbox activated for delivery, which they are the owner of, when communicating with the court. As a form of sanction for not doing so and as compensation for the higher amount of work connected to the processing of the submission and its annexes in paper form, a court fee of EUR 20 per filing including its annexes is imposed.

A part of the implementation of e-justice in Slovakia is also the implementation of electronic communication with various registers, such as the Business Register, the Trade Register or the Land Registry. The Business Register is the register is the longest online operating register and its electronicization was completed on 1 January 2020, which means that business entities can communicate with this register only electronically.

If we look at the implementation of e-justice within the EU, within the framework of the European Union, the European portal of e-justice – a central electronic site for the justice environment was created. It aims to make life easier for citizens by providing information on legal systems and improving access to justice across the EU in 23 languages. It covers many areas, for example, the impact of the Covid-19 pandemic on the field of justice, law and jurisprudence; justice systems; legal professions and justice networks; European judicial network for civil and commercial matters; legal assistance, filing in court, mediation; tools for courts and court officers; registers; European professional judicial training and European judicial atlas in civil matters.

In general, we can say that the launch of the complete functioning of e-justice should facilitate access to courts, facilitate the work of judges and court officers, as well as speed up court proceedings.

8 Slovak e-government from the user´s point of view

The theoretical and legal background for the implementation of e-government is an important precondition. Nevertheless, we assume that it is important to make a few notes about its actual usage, not only from the perspective of application issues (and problems), that were already mentioned in the above text but also from rather a statistical and user-assessment point of view.

As regards the elementary precondition for the usage of electronic services of the Government – access to the Internet – according to the Statistical Office of the Slovak Republic (2023: 4), 90.6% of households (out of a total of 1.720.474 households) have Internet access available. There are differences among the households in different regions of Slovakia, though. The best results were achieved in the Bratislava region (95.7%) and the worst in the Nitra region (84.7%). In 2022, 89.1% of the population used the Internet within the last 3 months.

Quite complex statistics on the use of e-government are provided by NASES through the free-accessible Open Data Portal (data.gov.sk). The portal was prepared in connection with the Open Data Partnership program more than 10 years ago. In 2012, the government approved an action plan for open governance, based on which this portal was created and where the public authorities should publish data acquired within their activities. Šebesta et al. (2020: 20), however, conclude that the published number of datasets as well as the organizations that publish the data on the portal is in their view extremely low[12], while at the same time, it is difficult to estimate its reason (the authors believe that this might be attributable to understaffing in the field of data acquisition and processing and, perhaps, unawareness of the obligation to publish this data).

From these statistics (data.gov.sk, 2023) we can learn that a total of 10.888 public authorities (including state bodies, towns and municipalities, courts, notaries, bailiffs, public schools, etc.) have already activated their electronic mailboxes and provide 252.428 specific e-forms and electronic services. Out of these, 10.533 public authorities have made available at least the service of the so-called general agenda. As for the status of integration of projects into the CPAP (Slovensko.sk), currently 360 public authorities are either in the process of realisation – deployment (278 – mostly towns and municipalities) or its preparation (35) and other legal entities (150) are in the process as well.

As for the users of the public e-services, an electronic mailbox was established for 5.565.143 natural persons and 1.611.665 legal entities (starting in 2014), however, out of them, only 262.958 mailboxes of natural persons and 505.578 mailboxes of legal persons[13] have already been activated (i.e. used) by them (in 2023). This represents 31.4% for legal persons (where the share might be higher taking regard to the meanwhile defunct companies) but only 4,73% for natural persons (data.gov.sk, 2023). This

corresponds to the data provided by the Statistical Office of SR (2023: 17 et seq.) on the interactions of persons who used the Internet within the last 12 months (3 754 739) with public authorities. While up to 62% of individuals (respondents) used the websites of public institutions as a data source in 2023, the specific use of electronic services was minimally represented (individual submission of tax returns 8.8%, requesting official documents 10.6%, submitting applications for cash benefits or other claims 10.0 %, submitting any other applications, complaints, or assertion of claims 3.4%). Most frequent reasons were the lack of skills or knowledge with 5.2%, missing electronic signature or electronic ID card or not activated electronic identifier (5,5%), representation (3.6%) and security concerns (3.6%). Of the same number of people, 12.9% used the electronic identity card to access online services for private purposes. Of these, up to 70.6% used the card for services provided by the state administration (e.g. filing a tax return, applying for social benefits, applying for official certificates, accessing health records, etc.) and 43.1% for services provided by the private sector. According to the European Commission (2022: 14) almost four million people (or almost 72% of the citizens) already have an eID. Thus, the level of actual usage of these electronic identifiers is very low.

In 2022, there were a total of 29.264.888 electronic mailbox logins with the predominance of legal entities (53,4%) over the public authorities (32.1%) and natural persons (14,5%). The total number of submissions was 1.148.588 and 11.093.244 decisions were issued (delivered). The total number of business transactions[14] was 14.503.856 and 53.852.168 technical messages was delivered (data.gov.sk, 2023). The amount of electronic communication acting is presumably dependent on the compulsory communication of some persons (especially legal counsels, legal entities and entrepreneurs) with public administration bodies in specific but very frequent cases, such as tax and customs issues, court proceedings, but also the availability of such communication, e.g. with social insurance and health insurance companies.

A lower quantity of electronic communication on the side of natural persons is visible and may be, from the viewpoint of the authors and their personal experience, attributable to the low user-friendliness of the system applicable. Especially in the beginning of the implementation of e-government, the legislation was rather perplexing, the technical level of the services was low (causing many technical errors and system outages), the establishment of the e-communication (required physical visiting of the particular authority´s office) was inconvenient, moreover, some of the submissions needed to be supplemented also in the paper form, and the multiplicity of electronic portals (one general of Slovensko.sk alongside special portals for tax administration, social insurance company, health insurance companies, public procurement, paying the toll, etc.), which is still present, might be confusing and impractical. The current situation is improved in some aspects, but not all of the shortcomings have already been addressed. The DESI index (digital economy and social index) of Slovakia with an overall 43.4 (out of 100) points (in 2022) is below the EU average and, among the EU states, we reached the fifth

rank from the end and, as regards the digital public services[15] solely, with a score of 52 we reached the fourth rank from the end (European Commission, 2022).

A very similar assessment of the present-day status of e-government in Slovakia is presented by Šebesta et al. (2020, s. 75-76) who depict four main reasons for relatively badly perceived practical usage of e-government in Slovakia, which may also serve as the proposals of areas that need to be tackled and improved: the user-unfriendly portal Slovensko.sk, the complexity and incomprehensibility of the legal regulations based on which e-government services are provided, low computer skills of employees in public administration and inconsistent use of the once-only principle. They assume that many electronic services provided by specific authorities are often suitable only for professionals who deal with consulting services in the given field and are too complicated for non-professional users. Similar evaluation is mentioned in the Report on the status of e-government in Slovakia, which speaks of low user-comfort, especially when encountering various public authorities, where users encounter mutual incompatibility of the visual appearance and vocabulary of the services, the logic of their use, but still also the problems of the portability of the formats used and the feedback from the users is insuffieciently dealt-with (Slovensko.Digital, 2020: 9). These assumptions may be supported by the research of Laitkep, Jaculjaková and Štofková (2021: 61), who found that more than half (56%) of companies who need various statements or extracts available through the Slovak Postal Office (e.g. extract from the commercial register, extract from the title deed, extract from the criminal record), they prefer to do it via postal office rather than Slovensko.sk.

The trend in the use of e-government by individuals is yet (at least slowly) growing. Research by Madleňáková and Madleňák (2012: 63, 64) from 2012 shows that, compared to 2007, the proportion of respondents preferring the Internet to other means of communication with public administration bodies increased from 11% to 27%, and in 2012, such a service was used at least once by 72% of respondents. According to Eurostat, between 2012 and 2021 the share of individuals who used the internet for interaction with public authorities grew in the criterion "submitting the completed forms" (from a minimum of 13.14% in 2015 to 25.17% in 2021), but as for interaction with public authority (in general), the trend is very moderate yet growing (but with regular fluctuations), reaching minimum in 2013 (32,72%), maximum in 2020 (61.84%) and the latest value of 55.95% (in 2021).

As the European Commission (2022: 4) concludes, progress has been made, but the country needs to continue its efforts to improve and expand digital public services. We already can see e.g. the improvement of the range of services available – practically all the spheres of public administration have the electronic services available (Slovensko.Digital, 2020: 10, the elimination of technical problems connected with the usage of the portal Slovensko.sk[16], elimination of many formerly-requested duplicate paper-forms of electronically submitted documents, elimination of dual delivery in excise

duties cases (to Slovensko.sk and portal of financial administration) and shifting the communication agenda purely to the portal Slovensko.sk (since 2022), and many other steps to enlarge the scope of e-agenda and improve its user comfort. Also of great importance was the adoption of Act No. 177/2018 Coll. on some measures to reduce the administrative burden by using public administration information systems and on the amendment of some laws (the so-called Anti-Bureaucracy Act), according to which public bodies are obliged and authorized to obtain and use data already registered in public administration information systems in their official activities and to provide this data to each other free of charge to the extent necessary and thus reduce the range of data required from users-clients[17]. The National Concept of Informatization of the Public Administration for years 2021-2026', approved by the Slovak Government in December 2021, outlines the strategy for more reliable and user-friendly digital public services, which will be most welcome.

9 Conclusions

The trend of implementation of e-government in the countries worldwide is unquestionable. Slovakia started its journey around 2000 when the first conceptual and strategic documents and pioneer pieces of legislation began to be adopted. Nevertheless, it is actually only in the last 10 years when the level of e-government in Slovakia started its modern development and began to be implemented in a more complex manner. The current legislative framework is adequately thorough and complex to create all the preconditions to accommodate the needs of the modern digital era, yet, the level of the practical use of e-government services is not at the desired level. A large share of private entities (especially legal persons and entrepreneurs) have been forced to communicate electronically with public authorities to spare the administrative costs of public administration and streamline the processes safeguarded by the state, even though, many of them preferred this way of communication even voluntarily. The same demands are not burdening the individuals, where we encounter a laxer approach in the use of already available public e-services. With each passing year, even this target group is slowly adjusting to the modern ways of dealing with state or municipal relations, though. This is, in our point of view, definitely attributable to the improved level of e-government services from the viewpoint of its range and user comfort, as well. Still, a lot needs to be done in this regard and despite not being yet on as high a level as many neighbouring countries or other EU countries are, there is visible progress and we believe that further development of Slovak e-government´s level will aim at better achievements in the following period.

Acknowledgment:

This research was supported by grant projects APVV-24-0171 (Digital balance – moderating illegal content and resolving disputes on digital platforms), VV-MVP-24-0038 (Analysis of liability for Internet torts with machine learning methods), APVV-21-0336 (Analysis of Judicial Decisions using Artificial Intelligence) and APVV-23-0158 (Customs union reform in the period of e-commerce in the Slovak Republic).

Notes:

[1] In Slovakia, savings of the Central Public Administration Portal according to the validated Cost Benefit Analysis (CBA) per shipment amount to EUR 4.28 (Slovensko.sk, 2023).
[2] A detailed process of implementation of e-government in Slovakia is provided by Sopúchová (2021: 33 et. seq.)
[3] As for the attachments to their filings, even these four categories of entities are allowed to deliver them by other than electronic means.
[4] E.g. the portal of the Tax Administration could not read the guaranteed electronic signature on the filing by the taxpayer, see Judgement of the Supreme Court of Slovak Republic of 29 October 2012, case No. 5Sžf/77/2011.
[5] Application problems and confusion of tax subjects (and their representatives) regarding the correct use of procedures for electronic submissions and their duties there-to related are also evident from the decision-making activity of the courts, when they discussed proposals in proceedings on protection against illegal intervention by public administration bodies, or their inaction, nevertheless, always with a negative conclusion for the application. See, e.g.: Judgment of the Regional Court in Bratislava of 21 November 2014, case No. 6S/115/2014; Resolution of the Regional Court in Žilina of 24 June 2015, case No. 21S/43/2015; Regional Court in Bratislava of 21 November 2014, case No. 6S/126/2014; Resolution of the Constitutional Court of the Slovak Republic of 13 August 2014, case No. I. ÚS 411/2014-11. (Románová, Červená, 2015).
[6] See Judgement of the Supreme Court of Slovak Republic of 4 November 2015, case No. 4Sžnz/1/2015.
[7] Judgement of the Supreme Court of Slovak Republic of 13 September 2016, case No. 5 Sžf 88/2014.
[8] Even though, a longer outage of the portal was recorded in July 2022 and lasted for more than one day (DSL.sk, 2022).
[9] And eventually by the tax administrator´s employee, if feasible and expedient.
[10] Such an option is directly available in the electronic mailbox.
[11] For detailed information on the DCOM project and the development and challenges of electronicization at the municipal level see Červená, Románová (2016) and Románová, Červená (2017) and (2019).
[12] As of 20 November 2023, it was only 3.415 datasets of 100 organisations (most of them submitted by the Statistical Office of SR) with 10.367 users (data.gov.sk, 2023).
[13] There were several rounds of automatic activation of electronic mailboxes of legal persons and entrepreneurs (starting with those registered in the commercial registry in 2018 and following in June 2020 with other non-business entities like foundations, non-profit organizations, churches or political parties).
[14] Comprising completed submissions, decisions, notifications, and saving the message in the pending/sent messages.

[15] The number of e-government users of all Internet users is 62% (and descending), pre-filled forms: 45 points (out of 100), Digital public services for citizens: 65 points (out of 100), Digital public services for businesses: 75 points (out of 100), open data: 50% (European Commission, 2022: 13).
[16] In 2019, there were 29 outage situations and in 2020 even as many as 185 situations, while only 15 in 2021 and 9 in 2022 (Data.gov.sk, 2023).
[17] Which, however, does not necessarily apply to all the public authorities, thus, not all the situations are already covered by this once-only approach (Slovensko.Digital, 2020: 14).

Bibliography

Andraško, J., et al. (2022) *Regulačné výzvy e-governmentu v Slovenskej republike v kontexte práva Európskej únie* (Prague: Wolters Kluwer).

Bajgar, A. (2024) *Kybernetická bezpečnost orgánů veřejné správy (Master's thesis)* (Brno: Masaryk University, Faculty of Law).

Banaszak, B. (2009) *Konstytucja Rzeczypospolitej Polskiej. Komentarz* (Warsaw: CH. Beck).

Baranyi, B. (2018) A kapcsolattartás általános szabályai, In: Baranyi, B, Barabás, G. & Fazekas, M (eds.) *Kommentár az általános közigazgatási rendtartásról szóló törvényhez* (Budapest: Wolters Kluwer Hungary), pp. 234-241.

Baranyi, B., Homoki, P. & Kovács, A. T. (2018) *Magyarázat az elektronikus ügyintézésről* (Budapest: Wolters Kluwer Hungary).

Bencsik, A. (2024) The Opportunities of Digitalisation in Public Administration with a Special Focus on the Use of Artificial Intelligence, *Studia Iuridica Lublinensia*, 33(2), pp. 11-23, https://doi.org/10.17951/sil.2024.33.2.11-23.

Bencsik, A. & Karpiuk, M. (2023) Cybersecurity in Hungary and Poland. Militaryaspects, *Cybersecurity and Law*, 9(1), pp. 80-94, https://doi.org/10.35467/cal/169302.

Bencsik, A., Karpiuk, M. & Strizzolo, N. (2024) Cybersecurity of E-government, *Cybersecurity and Law*, 11(2), pp. 146-160, https://doi.org/10.35467/cal/188565.

Bohatá, M. (2020) *Zpráva ke stavu veřejné správy červenec–prosinec 2020* (Praha: Síť k ochraně demokracie).

Bowman A. O'M. & Kearney R. C. (2016) *State and Local Government* (Wadsworth, Boston (MA, USA): Wadsworth Publishing).

Brůna, et al. (2005) *Veřejná správa v České republice* (Praha: Ministry of the Interior of the Czech Republic).

Červená, K. & Románová, A. (2016) E-government v miestnej štátnej správe a samospráve na Slovensku, *Právo, obchod, ekonomika*, VI, pp. 115-124, (Košice: Pavol Jozef Šafárik University in Košice).

Chałubińska-Jentkiewicz, K. & Karpiuk, M. (2015) *Prawo nowych technologii. Wybrane zagadnienia* (Warsaw: Wolters Kluwer).

Chałubińska-Jentkiewicz, K., Karpiuk, M. & Kostrubiec, J. (2021) *The Legal Status of Public Entities in the Field of Cybersecurity in Poland* (Maribor: Institute for Local Self-Government Maribor), https://doi.org/10.4335/2021.5.

Csatlós, E. (2024) Hungarian administrative processes in the digital age: An attempt to a comprehensive examination, *Intersections - EEJSP*, 10(1), pp. 189–209, https://doi.org/10.17356/ieejsp.v10i1.1250.

Czudek, M. (2022) *Future Plans for Development of Czech Civil Service*, 15 October 2024, available at: https://reform-support.ec.europa.eu/document/download/b79c0317-5182-42e2-82f7-57a8a4bfd930_en?filename=Session%205.%20Priorities%20for%20CZ.pdf (September 25, 2025).

Czuryk, M. (2019) Supporting the development of telecommunications services and networks through local and regional government bodies, and cybersecurity, *Cybersecurity and Law*, 2(2), pp. 39-50, https://doi.org/10.35467/cal/133839.

Czuryk, M. (2022a) Restrictions on the Exercising of Human and Civil Rights and Freedoms Due to Cybersecurity Issues, *Studia IuridicaLublinensia*, 31(3), pp. 31-43, https://doi.org/10.17951/sil.2022.31.3.31-43.

Czuryk, M. (2022b) Special rules of remuneration for individuals performing cybersecurity tasks, *Cybersecurity and Law*, 8(2), pp. 105-112, https://doi.org/10.35467/cal/157128.

Czuryk, M. (2023) Cybersecurity and Protection of Critical Infrastructure, *Studia Iuridica Lublinensia*, 32(5), pp. 43-52, https://doi.org/10.17951/sil.2023.32.5.43-52.

Data.gov.sk (2023) *Datasets by: The National Agency for Network and Electronic Services (NASES)*, available at: https://data.gov.sk/dataset?_organization_limit=0&organization=8155f071-182e-4c85-b6a0-32bf69399b17&page=2 (November 20, 2023).

DCOM (Dátové Centrum obcí a miest) (2023), available at: https://www.dcom.sk/ (November 10, 2023).

DSL.sk (2022) *Štát po dlhom výpadku Slovensko.sk radí ľuďom čo pri zmeškaní lehôt*, 16 August 2022, available at: https://www.dsl.sk/article.php?article=26422&title= (November 20, 2023).

Dušek, J. (2023) Data Boxes as a Part of the Strategic Concept of Computerization of Public Administration in the Czech Republic, *Administrative Sciences*, 13(6), p. 154, https://doi.org/10.3390/admsci13060154.

eGov.sk (2008) *Elektronická verejná správa*, available at: http://info.egov.sk/node/90 (October 20, 2023).

European Commission (2022) *The Digital Economy and Society Index (DESI): Slovakia*, available at: https://digital-strategy.ec.europa.eu/en/policies/desi-slovakia (November 21, 2023).

Evans, M. C., Cates, C. L. & McIntosh, W. V. (2015) The Reality of Jurisprudence(?): Interpretive Methods in the Opinions of Justices Antonin Scalia and Stephen Breyer, *Justice System Journal*, 36(1), pp. 20-48, https://doi.org/10.1080/0098261X.2014.969853.

Fiala, Z. & Sovova, O. (2020) *New challenges for public administration at the age of the right to internet access*, Conference Paper, https://doi.org/10.31410/EMAN.2020.201.

Frimmel, M. (2002) *Elektronický obchod* (Prague: Prospektum).

Gaie, C. & Karpiuk, M. (2024) The Provision of e-Services by Public Administration Bodies and Their Cybersecurity, In: Gaie, C. & Mehta, M. (eds.) *Transforming Public Services—Combining Data and Algorithms to Fulfil Citizen's Expectations* (Cham: Springer), pp. 175-188, https://doi.org/10.1007/978-3-031-55575-6_7.

Heeks, R. (2006) *Implementing and Managing E-Government* (London: SAGE Publications), https://doi.org/10.4135/9781446220191.

Hoffman, I. & Cseh, K. B. (2020) E-administration, Cybersecurity and municipalities – the challenges of cybersecurity issues for the municipalities in Hungary, *Cybersecurity and Law*, 2(2), pp. 199-211.

Hučková, R. & Treščáková, D. (2017) Nariadenie eIDAS - riešenie pre odstránenie nedôvery v elektronické obchodovanie?, *Právo, obchod, ekonomika*, VII., pp. 201-210, (Košice: Pavol Jozef Šafárik University in Košice).

Jeong, C. H. (2007) *Fundamental of Development Administration* (Selangor: Scholar Press).

Kačaljak, M. (2017) V*ybrané trendy vo výbere daní a možnosti ich právnej reflexie na Slovensku* (Bratislava: Wolters Kluwer).

Kaczmarek, K. (2019) Zapobieganie zagrożeniom cyfrowym na przykładzie Republiki Estońskiej i Republiki Finlandii, *Cybersecurity and Law*, 1(1), pp. 143-157, https://doi.org/10.35467/cal/133778.

Karpiuk, M. (2021a) Cybersecurity as an element in the planning activities of public administration, *Cybersecurity and Law*, 5(1), pp. 45-52, https://doi.org/10.35467/cal/142179.

Karpiuk, M. (2021b) Organisation of the National System of Cybersecurity: Selected Issues, *Studia IuridicaLublinensia*, 30(2), pp. 233-244, https://doi.org/10.17951/sil.2021.30.2.233-244.

Karpiuk, M. (2021c) The Local Government's Position in the Polish Cybersecurity System, *Lex Localis – Journal of Local Self-Government*, 19(3), pp. 609-620, https://doi.org/10.4335/19.3.609-620(2021).

Karpiuk, M. (2022a) Cybersecurity-related responsibilities of the minister competent for computerization, *Cybersecurity and Law*, 8(2), pp. 17-26, https://doi.org/10.35467/cal/157120.

Karpiuk, M. (2022b) Tasks of the Minister of National Defense in the area of cybersecurity, *Cybersecurity and Law*, 7(1), pp. 85-94, https://doi.org/10.35467/cal/151816.

Karpiuk, M. (2022c) The Competence of the Internal Security Agency in Protecting the Security of Communication and Information Systems and Networks of Public Administration Authorities, In: Karpiuk, M. & Kostrubiec, J. (eds.) *The Public Dimension of Cybersecurity* (Maribor: Institute for Local Self-Government Maribo), pp. 69-78, https://doi.org/10.4335/2022.1.7.

Karpiuk, M. (2022d) The Protection of State Security in Cyberspace as a Justifying Ground for Restricting Constitutional Freedoms and Rights, *Przegląd Prawa Konstytucyjnego*, 3, pp. 401-412, https://doi.org/10.15804/ppk.2022.03.30.

Karpiuk, M. (2023) The executive agency as a legal organisational form of implementing cybersecurity tasks, *Cybersecurity and Law*, 9(1), pp. 48-60, https://doi.org/10.35467/cal/169298.

Karpiuk, M. & Chałubińska-Jentkiewicz, K. (2015a) *Informacja i informatyzacja w administracji publicznej* (Warsaw: AON).

Karpiuk, M. & Chałubińska-Jentkiewicz, K. (2015b) *Prawo bezpieczeństwa informacyjnego* (Warsaw: AON).

Karpiuk, M. & Kelemen, M. (2022) Cybersecurity in civil aviation in Poland and Slovakia, *Cybersecurity and Law*, 8(2), pp. 70-83, https://doi.org/10.35467/cal/157125.

Kolbenhayerová, K. & Homa, T. (2022) Digitalization in public administration and its trends, *Institutiones Administrationis – Journal of Administrative Sciences,* 2(1), pp. 24–35, https://doi.org/10.54201/iajas.v2i1.24.

Laitkep, D., Jaculjaková, S. & Štofková, J. (2021) Využívanie služieb e-governmentu prostredníctvom slovenskej pošty, *Pošta, Telekomunikácie a Elektronický obchod*, 16(2), pp. 56-62, https://doi.org/10.26552/pte.C.2021.2.9.

Layne, K. & Lee, J. (2001) Developing fully functional E-government: A four-stage model, *Government Information Quaterly,* 18(2), pp. 122-136, https://doi.org/10.1016/S0740-624X(01)00066-1.

Lechner, T. (2013) *Elektronické dokumenty v právní praxi* (Prague: Leges).

Macková, A., Vaníček, Z. & Štědroň, B. (2008) *Vybrané právne a technické aspekty elektronizácie agend verejnej správy v Európskej únii* (Bratislava: Magnet Press Slovakia).

Madleňáková, L. & Madleňák, R. (2012) Analýza využívania služieb egovernmentu v SR, *Pošta, Telekomunikácie a Elektronický obchod*, 7(2), pp. 58-69, https://doi.org/10.26552/pte.C.2012.2.9.

Maisner, M. & Vlachová, B. (2015) *Zákon o kybernetické bezpečnosti - komentář* (Praha: Wolters Kluwer).

Mates, P. & Smejkal, V. (2012) *E-government v České republice: Právní a technologické aspekty* (Prague: Leges).

Mezei, K. & Träger, A. (2025) Risks and Resilience in the European Union's Regulation of Online Platforms and Artificial Intelligence: Hungary in Digital Europe, In: Gárdos-Orosz, F. (ed.) *The Resilience of the Hungarian Legal System since 2010* (Cham: Springer), pp. 143-158, https://doi.org/10.1007/978-3-031-70451-2_9.

Ministry of Finance of Slovak Republic (2008) *Národná koncepcia informatizácie verejnej správy* (Bratislava: Ministry of Finance of Slovak Republic).

Polčák, R. (2014) *Nařízení eIDAS*, available at: http://ict-law.blogspot.sk/2014/09/narizeni-eidas.html (July 18, 2025).

Polčák, R., et al. (2018) *Právo informačních technologií* (Praha: Wolters Kluwer ČR).

Romaniuk, P. (2022) Szanse i zagrożenia dla administracji publicznej w świadczeniu usług drogą elektroniczną, *Studia Prawnoustrojowe*, (58), pp. 437-454, https://doi.org/10.31648/sp.8055.

Románová, A., Červená, K. (2015) Niekoľko poznámok k elektronizácii správy daní, *Právo, obchod, ekonomika*, V, pp. 329-335 (Košice: Pavol Jozef Šafárik University in Košice).

Románová, A. & Červená, K. (2016) Elektronická komunikácia podnikateľov s verejnou správou (právne aspekty), *Current Problems of the Corporate Sector 2016* (Bratislava: EKONÓM), pp. 865-875.

Románová, A. & Červená, K. (2017) E-Government na Slovensku z pohľadu územnej samosprávy, *Právo, obchod, ekonomika*, VII, pp. 271-280 (Košice: Pavol Jozef Šafárik University in Košice).

Románová, A. & Červená, K. (2017) Implementation of e-Government in the Slovak Republic at the Level of Local self-Government, *Proceedings of the 17th European*

Conference on Digital Government (Reading: Academic Conferences and Publishing International), pp. 170-178.

Románová, A. & Červená, K. (2019) Computerisation of Public Administration in Slovakia - Impact on (the Fiscal Position of) Municipalities, *Public Governance, Administration and Finances Law Review: in the European Union and Central and Eastern Europe*, 4(1), pp. 26-43.

Ščerba, T. (2009) Some questions on the act no. 300/2008 – e-government act, *Masaryk University Journal of Law and Technology*, 3(3), pp. 401-414.

Šebesta, J., Braxator, T., Láni, R. & Kopčaková, S. (2020) *eGovernment a jeho vplyv na podnikateľský sektor*, available at: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://fsr.gov.sk/wp-content/uploads/2022/09/eGovernment_a_jeho_vplyv_na_podnikatelsky_sektor-1.pdf?csrt=173032037514585017 (November 20, 2023).

Skóra, A. (2022) O rewolucji w zakresie e-doręczeń raz jeszcze. Uwagi na tle art. 6 ustawy o doręczeniach elektronicznych, *Studia Prawnoustrojowe*, (58), pp. 473-490, https://doi.org/10.31648/sp.8342.

Slovensko. Digital (2020) *Správa o stave slovenského eGovernmentu*, available at: https://sprava.slovensko.digital/ (November 10, 2023).

Slovensko.sk (2023) *Štatistika Slovensko.sk*, available at: https://www.slovensko.sk/sk/statistika-slovensko-sk (November 24, 2023).

Smejkal, V., Kodl, J. & Uřičař, M. (2015) Elektronický podpis podle nařízení eIDAS, *Revue pro právo a technológie*, 6(11), pp. 189-235.

Sopúchová, S. (2021) *Informatizácia verejnej správy, e-Governmnet* (Bratislava: Komenský university, Faculty of Law).

Špaček, D. (2012) Trends of E-government in Czech Municipal and Regional Self-Government, *Review of Economic Perspectives – Národohospodářský obzor*, 12(1), pp. 42–67, https://doi.org/10.2478/v10135-012-0003-9.

Statistical Office of Slovak Republic (2023) *Survey on Information and Communication Technologies Usage in Households 2023*, available at: https://slovak.statistics.sk (December, 2023).

Štědroň, B. (2007) *Úvod do eGovernmentu v České republice: právní a technický průvodce* (Praha: Úřad vlády České republiky).

Studýnka, T. (2019) *Kybernetická bezpečnost ve veřejné správě (LL.M. thesis)* (Brno: Masaryk University, Faculty of Law).

Švadlena, P. & Švecová, Ž. (2023) *Elektronické právní jednání v soukromoprávních vztazích,* October 14, 2024, available at: https://www.epravo.cz/top/clanky/elektronicke-pravni-jednani-v-soukromopravnich-vztazich-116740.html#:~:text=910%2F2014%20(dále%20jen%20„důvodu%2C%20že%20má%20elektronickou%20podobu (May 25, 2025).

Treščáková, D. (2017) Virtuálna identita a elektronické schránky - vzájomné súvislosti, *Studia Iuridica Cassoviensia*, 5(1), pp. 113-120.

Treščáková, D. (2021) *Právo elektronického obchodu. Širšie súvislosti* (Prague: Leges).

Uhlířová, J. (2012) *Egovernment v České Republice* (Brno: Masarykova Univerzita).

Veselý, A., Nekola, M. & M. Hejzlarová, E. (2016) *Policy Analysis in the Czech Republic* (Bristol: Policy Press).

Wachter, S., Mittelstadt, B. & Russell, C. (2018) Counterfactual explanations without opening the black box: automated decisions and the GDPR, *Harvard Journal of Law & Technology*, 31(8), pp. 841-887, https://doi.org/10.48550/arXiv.1711.00399.

Winczorek, P. (2008) *Komentarz do Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 roku* (Warsaw: Liber).

Wohlers, T. E. (2010) Local E-Government Sophistication in the United States, In: Scholl H. J. (ed.) *E-Government: Information, Technology and Transformation* (London (UK); New York (NY, USA): Routledge), pp 89-106.

Institute for Local Self-Government Maribor

www.lex-localis.press
info@lex-localis.press