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.