

UDK: 35.072.2 : 004.3/.4 (437.6)

347 : 004.738.5 (437.6)

Review paper

Martin Friedrich, PhD student

Faculty of Law, Pavol Jozef Šafárik University in Košice, Slovakia

E-mail: martin@friedrich.sk

ORCID ID: 0009-0001-3775-8232

SLOVAK PRIVATE AND PUBLIC LAW IN DIGITAL SERVICES - A TENTATIVE ROMANCE*

ABSTRACT

The digitalization of public and private services in Slovakia has exposed significant discrepancies in adoption, regulation, and technological implementation. While private digital services, particularly e-commerce, have flourished, e-government services remain underutilized due to rigid legal frameworks, administrative burdens, and cyber security concerns. The requirement for Qualified Electronic Signatures (QES) in public services contrasts sharply with the more flexible use of electronic signatures in private transactions. Furthermore, inconsistencies between Slovak and European Union regulations on electronic signatures and digital identity have led to legal ambiguities that hinder seamless integration. Using a multidisciplinary approach that combines legal analysis, policy review, and case studies, the paper examines regulatory inconsistencies, barriers to private sector participation in public digital services, adoption of e-wallets, and the implications of security breaches, such as the recent large-scale ransom attack on public infrastructure. The findings highlight the urgent need for a more harmonized regulatory framework, greater cooperation between the government and private enterprises, and the adoption of user-friendly digital policies. The paper argues that Slovakia's digital transformation requires a shift toward more flexible authentication measures, enhanced cyber security strategies, and improved public trust in e-government services. By addressing these issues, Slovakia can achieve a more secure, efficient, and accessible digital ecosystem for both public and private sectors.

Keywords: e-government, electronic signatures, digital transformation, legal frameworks

1. INTRODUCTION

The objective of this paper is to explore the reasons behind the decline in the utilization of Slovak public electronic services, even during lockdowns, while the

proportion of online sales in Slovakia has consistently been above average compared to other member states.

Ideally, there would be no significant disparities in public and private legal frameworks, and technical solutions would be interoperable and platform-independent. For instance, a government authentication tool could serve as an identity proof in electronic commerce. Similarly, there should be no major differences in requirements regarding the proper type of electronic signature for a specific transaction.

By analyzing inconsistencies between Slovak private and public law and between Slovak and European regulation, we can comprehend the complex legal environment in which a user is situated. Considering that there are currently several types of valid electronic IDs from which older versions do not permit the creation of qualified electronic signatures, which are required in the majority of public services, we can understand why public electronic services can be confusing to use.

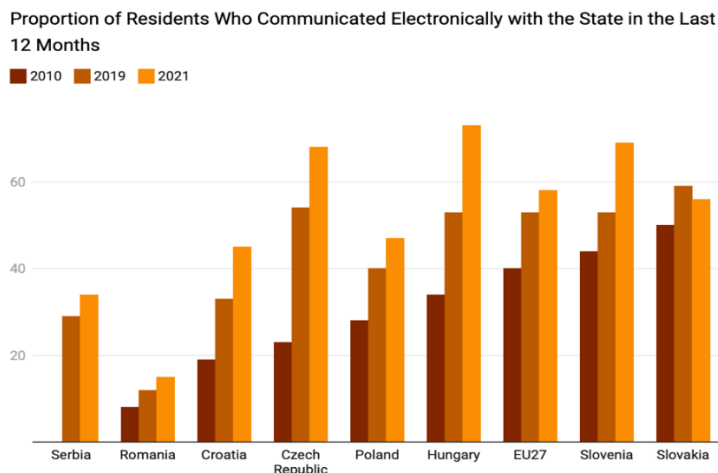
This paper delves deeper into the potential of recent initiatives, such as the streamlined process for establishing a limited liability company electronically and the introduction of national and European e-wallets, to bridge the gap between private and public electronic services. Nevertheless, the 2025 ransomware attack on the Slovak cadastral system, from which the cadaster's electronic services have yet to fully recover, has significantly eroded public trust in e-government. The aim of this paper is to contribute to the ongoing discourse on digital transformation by presenting empirical evidence and analytical insights specific to the Slovak context. By addressing the identified issues, the paper advocates for a more harmonized legal framework and, in the case of electronic public services, emphasizes the importance of predictability and transparency, which should result in increased confidence in electronic public services and their increased usage.

2. SLOVAKIA'S DIGITAL DILEMMA: PUBLIC VS. PRIVATE ADOPTION

The COVID-19 pandemic necessitated an accelerated digital transformation among governments, employers, and citizens. The United Nations identified this transformation as an opportunity for fostering digital inclusion and, in the long term, as a foundation for the advancement of innovative technologies such as

artificial intelligence (AI), block chain, robotics, and drone technologies.¹ Additionally, digitalization was seen as a means of enhancing the resilience of public services, healthcare, and economic systems. Several nations demonstrated remarkable adaptability in response to this challenge. For instance, governments in Latin America and the Caribbean implemented measures that led to an increase in government-related digital transactions from 21% prior to the pandemic to 39% during it. Nevertheless, the same study indicated that approximately 50% of citizens still completed their most recent transaction in person.² Comparable trends were observed in Central Europe. According to Erste Bank, the proportion of citizens who engaged in electronic communication with their respective governments between 2019 and 2021 increased in all countries except Slovakia.³

Chart No. 1: Proportion of Residents who communicated electronically with State in the last 12 months



Source: Denník N, proportion of citizens who engaged in electronic communication with their respective governments

* The paper was created as part of the research grant project VVSG No. 2024-3381, titled: Human Rights and Ethical Aspects of Digitalization and E-Commerce.

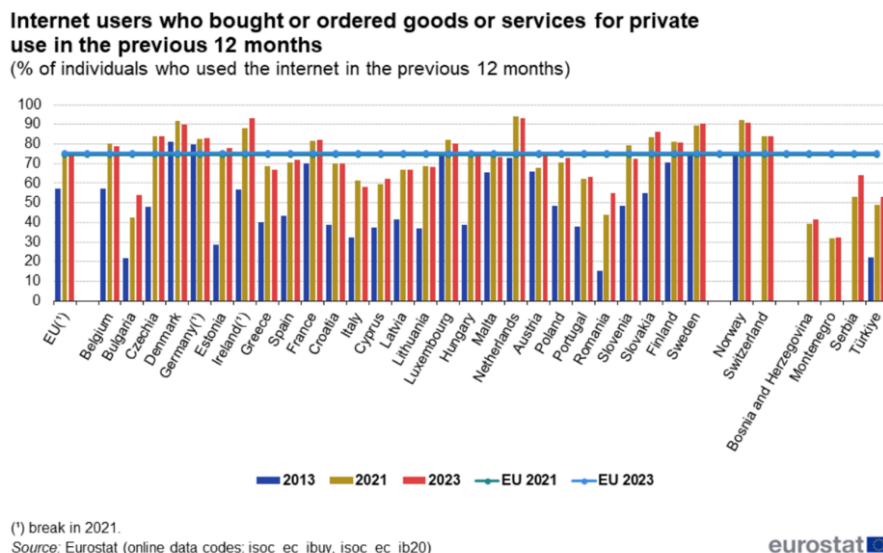
¹ COVID-19: Embracing digital government during the pandemic and beyond, UN. Department of Economic and Social Affairs, April 2020, <https://digitallibrary.un.org/record/3856978?v=pdf&ln=en>, 24 January, 2025.

² Roseth, B.; Reyes, A.; Yee Amézaga, K., *Public Services and Digital Government during the Pandemic: Perspectives of Citizens, Civil Servants, and Government Institutions*, Inter-American Development Bank, 2021, <http://dx.doi.org/10.18235/0003122>, 24 January, 2025.

³ Tomek, R., Graf dňa: RozširovanieGovernmentusavlaninaSlovenskuako v jedinejkrajineregiónuzastavilo,Denník N, N Press, s.r.o., 16. February 2022, <https://e.dennikn.sk/2724194/graf-dna-slovensko-sa-v-elektronickej-komunikacii-so-statom-prepadlo-pod-priemer-eu/>, 24 January, 2025.

Meanwhile, data from Eurostat (2023) reveal that 75% of internet users in the European Union engaged in online purchases or ordered services. In Slovakia, the proportion of online sales remained above the EU average.⁴

Chart No. 2: Internet users who bought or ordered goods or services for private use in the previous 12 months



Source: Eurostat, E-commerce statistics for individuals for 2023

These statistics underscore a significant discrepancy between private and public digital services in Slovakia. While the utilization of e-government services declined during the pandemic-induced lockdowns, e-commerce transactions exhibited a steady upward trajectory.

Through a multidisciplinary methodology that integrates legal analysis, policy evaluation, and case studies, this paper posits that the reasons for the statistical results can be attributed to two explanations.

This first explanation is based on the variations in the legal frameworks governing public and private regulation of electronic signatures significantly influences their

⁴ Eurostat, E-commerce statistics for individuals, https://ec.europa.eu/eurostat/statistics-explained/index.php?title=E-commerce_statistics_for_individuals#75_25_of_internet_users_bought_or_ordered_goods_or_services_online_in_the_EU_in_2023, 24 January, 2025.

application. The divergence in regulatory standards between public electronic services and private contractual use may result in unnecessarily strict limitations on the acceptable types of electronic signatures in public services, in contrast to the more flexible approaches adopted in comparable private-sector contexts.

Secondly, technical limitations, including inadequacies in state-issued electronic identification (e-ID) systems, have failed to meet user expectations. We argue that the Slovak government's shortcomings in providing timely and transparent communication regarding the hardware limitations of e-IDs, coupled with the implementation of opaque solutions—such as the distinction between qualified and advanced electronic signatures in certain cases—have led to an unnecessarily complex system for users.

This paper also argues that the Slovak government has been slow and selective in granting private enterprises access to specific government-provided digital services. For instance, certain businesses have been granted legal access to national identity databases, thereby gaining a competitive advantage in their services. The implementation of e-wallets based on European regulations could address this disparity. However, the Slovak government has opted for a distinct national e-wallet initiative, independent of the existing European framework, which is exclusively designed to serve law enforcement authorities.

Finally, we hypothesize that the aftermath of the most significant ransomware attack on public services in Slovak history may have a lasting impact on public trust in e-governmental services. Specifically, the inadequate communication regarding the incident, the extensive scope of its impact, and the prolonged duration of the disruption are likely to negatively influence public perception of e-governmental services.

3. REGULATION OF ELECTRONIC SIGNATURES

The legal framework governing electronic signatures is established by 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, 28.8.2014, p. 73–114 (hereinafter: eIDAS Regulation). At the national level, the eIDAS Regulation is further implemented through Act No. 305/2013 Coll. on the electronic execution of public authority powers (hereinafter: e-Government Act). The e-Government Act regulates the use of electronic signatures within public law. In the realm of private law, electronic signatures are governed by the Civil Code Act No. 40/1964 Coll. (hereinafter: Civil Code). Both the e-Government Act and the Civil Code are

supplemented by Act No. 272/2016 Coll. on Trust Services for Electronic Transactions in the Internal Market (hereinafter: Trust Services Act).

From a legislative perspective, a clear distinction exists between the regulation of public and private law concerning electronic signatures, which in itself does not present an issue. However, as this paper will illustrate, contradictions arise between the e-Government Act, the Civil Code, and the eIDAS Regulation regarding the use of electronic seals, the recognition of electronic signature types beyond qualified electronic signatures, and inconsistencies within the national framework. Before further analyzing these contradictions, it is necessary to define electronic signatures and seals and outline their various classifications.

3.1. Electronic signatures and the electronic seals

From a technical standpoint, an electronic signature and an electronic seal constitute data in electronic form that are attached to or logically associated with other electronic data for the purpose of authentication (Article 3 (10,25) of the eIDAS Regulation).

A distinction must be made between electronic signatures and digital signatures. Whereas an electronic signature is a legal concept defined by the eIDAS Regulation, a digital signature pertains to a mathematical and cryptographic method employed to create electronic signatures.⁵ According to ETSI TR 119 100, a digital signature is defined as *"data appended to, or a cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery."*⁶ Not all electronic signatures fall within the scope of digital signatures, necessitating differentiation between these concepts.

The eIDAS Regulation recognizes three types of electronic signatures:

- a) Qualified (QES),
- b) Advanced (AdES)
- c) Simple (SES).

Each of these signature types holds legal validity, with their primary distinction being the level of security provided.

⁵ eSignature FAQ, What is the difference between an electronic signature and a digital signature? European Commission, <https://ec.europa.eu/digital-building-blocks/sites/display/DIGITAL/eSignature+FAQ>, 27 January, 2025.

⁶ ETSI TR 119 001 V1.2.1 (2016-03), Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations, https://www.etsi.org/deliver/etsi_tr/119000_119099/119001/01.02.01_60/tr_119001v010201p.pdf, 27 January, 2025.

Chart No. 3: Relation between different types of electronic signatures and their security



The primary function of an electronic seal (ESeal) is to ensure the authenticity and integrity of an electronic document issued by a legal entity. The eIDAS Regulation defines an ESeal as *“data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter’s origin and integrity”* (Article 3 (25) of the eIDAS Regulation). Unlike electronic signatures, which signify an individual's intent, ESeals safeguard the integrity of documents issued by legal entities, whether public or private. Therefore, a document issued by a legal entity that represents a declaration of intent or an official decision must be electronically signed rather than merely sealed.

Both electronic signatures and electronic seals are created using similar technical methods. A QES and a Qualified Electronic Seal (QESeal) are both defined as an advanced electronic signature or seal created through a qualified electronic signature/seal creation device and based on a qualified certificate for electronic signatures (Article 3 (12,27) of the eIDAS Regulation).

A QES is the only type of electronic signature that holds the same legal effect as a handwritten signature (Article 25 (2) of the eIDAS Regulation). Other types of electronic signatures, including QESeals, do not possess this equivalent legal standing.

The creation of a QES or QESeal necessitates the fulfillment of all technical requirements, including the use of a certified qualified electronic signature/seal creation device, such as an e-ID chip card. The European Union maintains a

publicly available list of these qualified devices.⁷ Additionally, the QES/QESeal must be generated using a qualified certificate issued by a certified entity, also documented on the European Union's official registry.⁸

Compared to QES/QESeal, advanced electronic signatures (AdES) and advanced electronic seals (AdEseal) are either missing a qualified electronic signature/seal creation device or a qualified electronic signature/seal certificate. Although these types of signatures and seals offer a lower level of security compared to QES/QESeal, they remain valid and provide a reasonable degree of trustworthiness.

The Simple Electronic Signature (SES) is the most commonly utilized form of electronic signature. Examples of SES include an email sender's name, click-wrap or scroll-wrap agreements in e-commerce⁹, and various forms of digital communication such as messaging applications. Although SES is the least secure form of electronic signature, this does not inherently render documents signed using SES invalid. However, due to its lower security threshold, legal acts signed with SES may be more susceptible to challenges regarding authenticity. As will be demonstrated in subsequent sections, Slovak courts have historically exhibited reluctance in recognizing SES as a legally valid expression of will and have often required QES, despite the widespread use of SES by consumers and commercial entities.

4. QUALIFIED ELECTRONIC SIGNATURES VS. ADVANCED ELECTRONIC SIGNATURES IN E-GOVERNMENT

Until January 2024, Slovak residents could access public services exclusively through the use of Qualified Electronic Signatures (QES), which were required for the authorization of submitted filings. To generate a QES, users needed both a qualified electronic device and a qualified electronic certificate. Given that QES represents the highest and most secure form of electronic signature, it is evident why the government mandated its use. To facilitate compliance, the state issued

⁷ Qualified Signature/Seal Creation Devices and Secure Signature Creation Devices, European Commission, eIDAS Dashboard, <https://eidas.ec.europa.eu/efda/browse/notification/qscd-sscd>, 27 January, 2025.

⁸ EU/EEA Trusted List Browser, eIDAS Dashboard, <https://eidas.ec.europa.eu/efda/trust-services/browse/eidas/tls>, 27 January, 2025.

⁹ Treščáková, D., *Právoelektronickéhoobchodu, Širšiesúvislosti*. Praha: Leges, 2021, p. 62

electronic IDs (e-IDs) as qualified electronic devices, accompanied by qualified electronic certificates.

To promote the adoption of public e-services, the government designated certain services as exclusively electronic, such as the Register of Public Sector Partners, the Business Register, tax filings, and various judicial services, including initiating enforcement proceedings and submitting petitions for Reminder Proceedings. Additionally, the government mandated the use of e-government services for specific groups, including attorneys and legal entities. Consequently, this policy resulted in a substantial user base for QES, as individuals and businesses needed to utilize QES to continue their operations and meet legal obligations. It is important to note that QES generated by any qualified electronic device and qualified electronic certificate issued under the eIDAS Regulation must be accepted, with electronic IDs being the most prevalent among Slovak residents.

According to the Ministry of Interior of the Slovak Republic, between December 2013 and December 2024, the Slovak government issued a total of 5,329,419 e-IDs. In 2024 alone, 665,112 e-IDs (qualified electronic devices) and 109,935 qualified electronic certificates were distributed.¹⁰ This indicates that in 2024, only 109,935 Slovak residents opted to activate their QES, despite the availability of a free-of-charge qualified electronic certificate, which could be obtained online after the issuance of an e-ID.

This disparity can be attributed to the government's failure to address the expiration of e-ID integrated chips with sufficient foresight. Ultimately, this oversight compelled the government to waive the QES requirement for certain services and permit the use of Advanced Electronic Signatures (AdES). Unfortunately, determining which public services necessitate QES and which allow AdES remains a challenge for users.

On May 26, 2021, the Ministry of Interior issued a press release informing users that, within one month, the five-year certification of chips embedded in e-IDs would expire.¹¹ Users who had not downloaded a qualified certificate for

¹⁰Prehľad vydávania elektronických občianskych preukazov a certifikátov pre vytvorenie kvalifikovaného elektronického podpisu (eID štatistika) k 31.12.2024 (PDF, 200 kB), https://www.minv.sk/swift_data/source/policia/md_ode/eid_statistika/2024_eid_statistika/eID%20statistika_12.pdf, 30 January, 2025.

¹¹Platnosť certifikátu pre vydávanie e-podpisu a občianskych preukazoch a cudzineckých dokladoch končí 26. júna, používať vydané certifikáty však bude možné až do konca roku 2022, Ministry of Interior of the Slovak Republic, 26. 05. 2021 Press Release, <https://www.minv.sk/?tlacove-spravy&sprava=platnost-certifikatu-pre-vydavanie-e->

electronic signatures were granted a grace period until June 25, 2021, to obtain a new certificate. Failure to do so necessitated requesting a new e-ID for continued use of QES. Meanwhile, individuals possessing e-IDs issued before June 21, 2021, could generate QES until the end of 2022. However, from January 1, 2023, neither citizens nor legal residents with e-IDs issued before June 20, 2021, were able to create QES, effectively preventing their access to e-government services.

We contend that the government could have taken proactive measures to mitigate disruptions caused by the expiration of e-IDs. Initially, the public largely disregarded the issue, but as the deadline approached, it became apparent that individuals without a valid QES would be unable to file tax records or utilize e-government services. Reports from public media indicated that, in December 2022, applicants for e-IDs and residency cards faced extended waiting times merely to submit renewal applications. The Ministry of Interior confirmed that between December 1, 2022, and mid-January 2023, the state received over 130,000 applications for e-ID issuance. In December alone, 92,674 applications were submitted, and 54,341 ID cards were issued—three times the number issued in December 2021.¹² Furthermore, in December 2021, the government introduced new biometric e-IDs, cautioning that the transition to this technology would result in processing delays.¹³

By December 2022, it became evident that the government lacked the capacity to process the surge in e-ID renewal requests. As a result, in a last-minute decision, the government introduced Decree No. 511/2022 Coll. on December 19, 2022, allowing, for the first time, the use of AdES in electronic public services.¹⁴ This decree was initially intended as a temporary measure for individuals with e-IDs issued before June 20, 2021, who could no longer generate QES due to expired e-

podpisu-na-obcianskych-preukazoch-a-cudzineckych-dokladoch-konci-26-juna-pouzivat-vydane-certifikaty-vsak-mozne-az-do-konca-roku-2022, 2 February, 2025.

¹²Kosno, L., Žiadosti o nové e-občianske lámal rekordy. Štát tvrdí, že doklady doručivčas, Ringier Slovakia Media s.r.o., 18.1.2023, <https://zive.aktuality.sk/clanok/mpybc5l/ziadosti-o-nove-e-obcianske-lamali-rekordy-stat-tvrdi-ze-doklady-doruci-vcas/>, 2 February, 2025.

¹³Bezkontaktné biometrické občianske preukazy pre obyvateľov EÚ budú realitou. Ministerstvo vnútra pripravuje ich vydávanie, SITA Slovenská tlačová agentúra a.s., 17. 11. 2022, <https://sita.sk/bezkontaktno-biometricko-obcianske-preukazy-pre-obyvatelov-eu-budu-realitou-rezort-vnutra-pripravuje-ich-vydavanie/>, 2 February, 2025.

¹⁴Decree No. 511/2022 Coll. of the Ministry of Investments, Regional Development, and Informatization of the Slovak Republic on Recognized Methods of Authorization

ID chips.¹⁵¹⁶The provision was set to expire in June 2023, during which affected users were expected to obtain new e-IDs. However, given the significant number of individuals still in possession of expired e-IDs, the government repeatedly extended the expiration deadline—first to December 31, 2023, then to December 31, 2024, and most recently to December 31, 2025.¹⁷

The integration of AdES in public e-services could have facilitated greater innovation, including the development of remote electronic signatures and increased participation from private sector entities in e-governmental services. However, since AdES is regarded as a temporary measure, its implementation remains limited. At present, a total of 249 public services permit the use of AdES, yet identifying which services require QES versus AdES necessitates searching an Excel sheet¹⁸ on the National Agency for Network and Electronic Services' website.¹⁹ Given that the average public service user may lack the technical knowledge to differentiate between QES and AdES, the system remains unnecessarily complex.

Although both QES and AdES are theoretically available for use in electronic public services, their adoption has not resulted in substantive advancements in e-governmental services. The existence of 249 AdES-enabled services suggests an acknowledgment that not all public services require the stringent security of QES. Nevertheless, the lack of transparency regarding AdES implementation raises concerns. Presently, the primary benefit of permitting AdES in public services is that residents with e-IDs issued before June 20, 2021, are not compelled to obtain a new e-ID. However, this concession alone cannot be regarded as an innovation in digital governance.

¹⁵Kosno, L., Podpisujete sa e-občianskym starým typom? Dočasné riešenie má fungovať iba polrok, Ringier Slovakia Media s.r.o., 25.11.2022, <https://zive.aktuality.sk/clanok/zOxZBF1/podpisujete-sa-e-obcianskym-stareho-typu-docasne-riesenie-ma-fungovat-iba-polrok/>, 2 February, 2025.

¹⁶Vyhľadávka o uznaných spôsoboch autorizácie a nasadení zmeny, National Agency for Network and Electronic Services, <https://www.slovensko.sk/sk/institucie-formulare-a-ziado/vyhlaska-o-uznanych-sposoboch>, 2 February, 2025.

¹⁷Predĺženie používania uznaného spôsobu autorizácie, National Agency for Network and Electronic Services, 06. 11. 2024, https://www.slovensko.sk/sk/oznamy/detail/_predlzenie-pouzivania-uznaneho, 2 February, 2025.

¹⁸Vyhľadávka o uznaných spôsoboch autorizácie a zoznam služieb, National Agency for Network and Electronic Services, 30. 12. 2022, https://www.slovensko.sk/_img/CMS4/Zoznam_sluzieb_USA.xlsx, 2 February, 2025.

¹⁹Vyhľadávka o uznaných spôsoboch autorizácie a zoznam služieb, National Agency for Network and Electronic Services, 30. 12. 2022, https://www.slovensko.sk/sk/oznamy/detail/_vyhlaska-o-uznanych-sposoboch, 2 February, 2025.

4.1. Qualified electronic seals in public services

As previously stated, under the eIDAS Regulation, electronic seals serve as evidence that an electronic document has been issued by a legal entity, thereby ensuring the certainty of the document's origin and integrity (Article 3(25) of the eIDAS Regulation). However, pursuant to Section 23, Paragraph 1, Letter a) of the e-Government Act, Qualified Electronic Seals (QESeals) may be used to authorize electronic documents in the same manner as a Qualified Electronic Signature (QES). Consequently, there is no legal distinction between a public document signed using a QES or a QESeal, nor is there any difference if a legal entity signs a petition with either a QES or a QESeal.

When the Slovak Parliament enacted the e-Government Act in 2013, the accompanying Justification Report²⁰ asserted that an electronic seal is functionally equivalent to an electronic signature. Furthermore, it ambitiously claimed that the authorization of acts within the scope of the e-Government Act was fully aligned with the forthcoming eIDAS Regulation. However, with regard to electronic seals, this assertion is demonstrably inaccurate.

The authors of this paper are not privy to the rationale behind equating QES with QESeals in the e-Government Act. Given that this provision has remained unchanged since 2013, we infer that the intention was to streamline the administration of electronic public documents by permitting the use of QESeals without the additional requirement of a QES. However, since treating QESeals as equivalent to QES contravenes the eIDAS Regulation, we question the legality of the Slovak e-Government Act in this regard. Nevertheless, we are unaware of any legal precedent in which a public document electronically signed solely with a QESeal has been invalidated due to non-compliance with the eIDAS Regulation. However, it is crucial to acknowledge that Slovak public electronic documents retain legal validity across the European Union. If such documents are "signed" exclusively using QESeals, there is a risk that they may be rejected by receiving parties within the EU.

4.2. Mandate certificates in public services

Annex I of the eIDAS Regulation delineates the prerequisites for the issuance of qualified certificates for electronic signatures. Article 28, Section 3 of the eIDAS

²⁰Government Bill on the Electronic Form of the Exercise of Public Authority and on Amendments and Supplements to Certain Laws (e-Government Act), Explanatory Report – Special Part, <https://www.nrsr.sk/web/Dynamic/DocumentPreview.aspx?DocID=384288>, 2 February, 2025.

Regulation permits the inclusion of additional specific attributes in a qualified certificate, provided that such attributes are non-mandatory. Furthermore, these additional attributes must not compromise the interoperability and recognition of qualified electronic signatures across jurisdictions.

In the Slovak Republic, these ostensibly non-mandatory additional attributes have, in practice, been rendered obligatory. To facilitate the implementation of the eIDAS Regulation within Slovak national law, the legislature enacted Act No. 272/2016 Coll. on Trust Services for Electronic Transactions in the Internal Market and on Amendments and Supplements to Certain Acts (hereinafter: Trust Services Act). This statute introduced a distinct category of qualified certificate known as the "Mandate Certificate" (Section 8, Paragraph 1 of the Trust Services Act).

The Mandate Certificate diverges from a standard qualified certificate in that it incorporates supplementary attributes, including data facilitating the identification of the public body that the signatory, as a natural person, represents. The principal function of Mandate Certificates is to provide verifiable proof of the signatory's authorization to: (a) act on behalf of or in the name of the principal, (b) undertake activities in compliance with specific regulations, and (c) exercise functions stipulated under special regulations. Consequently, Mandate Certificates are issued to judges, attorneys, bailiffs, employees of public bodies, and other agents executing public duties.

Despite being a variant of a qualified certificate, the Mandate Certificate has been rendered mandatory for public authorities under the provisions of the e-Government Act (Section 23, Paragraph 1). This statutory requirement stipulates that: *"A public authority shall, in the exercise of public authority, authorize an electronic submission or an electronic official document using a qualified electronic signature created with a Mandate Certificate or a qualified electronic seal."* The imposition of this requirement raises concerns regarding its compliance with the eIDAS Regulation, as it appears to contravene its provisions by mandating a specific type of qualified certificate.

To facilitate the transition between paper-based and electronic documents, as well as vice versa, the e-Government Act introduced a procedural mechanism known as Guaranteed Conversion (Section 35 of the e-Government Act). This process enables the transformation of a document from one material form to another, specifically from paper to electronic format and vice versa. Additionally, Guaranteed Conversion accommodates the conversion of electronic documents in cases where an archival PDF format becomes obsolete. The legal significance of Guaranteed Conversion lies in the principle that the newly generated document retains the same legal effect and applicability for legal purposes as a certified copy

of the original document from which it was derived (Section 39, Paragraph 1 of the e-Government Act).

Given the legal ramifications of the Guaranteed Conversion process, its execution is entrusted exclusively to specific professions, including attorneys, notaries, banks, and postal service providers (Section 35, Paragraph 3 of the e-Government Act). Furthermore, Decree No. 70/2021 Coll. on Guaranteed Conversion prescribes that the authorization of this process must be executed using a Mandate Certificate.

The introduction and mandatory imposition of Mandate Certificates present a unique anomaly in the landscape of electronic signatures. At the national level, Mandate Certificates are treated as distinct from standard qualified certificates, despite their technical similarities. Moreover, their obligatory use by private entities in the context of Guaranteed Conversion exacerbates regulatory ambiguity. No compelling justification—compliant with the eIDAS Regulation—has been provided to explain why an attorney cannot utilize a standard qualified certificate to authorize the Guaranteed Conversion process. It is plausible that, as in the case of qualified electronic seals (QESeals), the primary purpose of Mandate Certificates is to streamline administrative procedures for public authorities. By requiring Mandate Certificates, public administration officials can efficiently verify the professional status of individuals such as attorneys, notaries, bailiffs, judges, and other public functionaries.

4.3. Electronic seals and signatures in private law

Electronic signatures and seals within the realm of private law are governed by Section 40, Paragraph 3 of the Civil Code. This provision stipulates that the written form of a legal act is preserved when such an act, performed via electronic means, is authenticated using a qualified electronic signature (QES) or a qualified electronic seal (QESeal).

4.4. Electronic seals

Similar to the application of QESeals in e-government services, the Civil Code permits the use of QESeals for electronic signatures in private law matters²¹. However, this stands in contradiction to the eIDAS Regulation, which explicitly

²¹Števček, M.; Dulak, A.; Bajánková, J.; Fečík, M.; Sedlačko, F., Tomašovič, M. a kol., *Občianskylákonník II. 2. vydání*. Praha: C. H. Beck, 2019, marg. č. 10, p. 321.

prohibits the use of electronic seals for the creation of electronic signatures. Another noteworthy peculiarity of the Civil Code is its failure to expressly restrict the issuance of electronic seals to legal persons, as mandated by Article 3 (24,25) of the eIDAS Regulation. Consequently, an individual unfamiliar with the eIDAS Regulation might incorrectly infer that: (a) electronic seals, particularly QESeals, can be utilized to create electronic signatures, and (b) any individual, rather than exclusively legal persons, can be issued electronic seals.

This discrepancy between the Civil Code and the eIDAS Regulation likely persists due to the limited practical application of electronic seals in private law matters. Since Slovak residents are issued qualified electronic certificates as part of their electronic identification (eID) or residency cards, there is no significant demand for separate electronic seals for legal persons. A company's managing director, for instance, can always utilize their personal qualified electronic certificate to generate a QES. This further supports the argument against the use of electronic seals for the creation of electronic signatures, as they do not confer any practical advantages over QES.

4.5. Electronic signatures

Regarding electronic signatures, two key issues warrant discussion: (1) the creation of QES and its equivalence to a notarized signature, and (2) the absence of national private law provisions recognizing advanced or simple electronic signatures.

4.6. Notarized signatures

Notarized signatures are either mandated by law or agreed upon by contracting parties. The primary significance of a notarized signature lies in the involvement of an impartial third party who verifies the identity of the signatory and confirms that the individual is alive and of sound mind at the time of signing. This verification enhances the credibility of the legal act recorded in the contract.

It remains debatable whether QES (or QESeals) can achieve the same level of credibility as a notarized signature. Unlike notarized signatures, the creation of a QES does not necessitate the presence of an independent third party. Instead, under Section 40, Paragraph 5 of the Civil Code, an electronic time stamp must be appended to the electronic signature for it to have the same legal effect as a notarized signature. The purpose of this time stamp is to verify the exact moment

of QES creation. However, the Civil Code does not specify when the time stamp should be applied to the QES.

In the domain of public electronic services, if an electronic signature is to have the effect of a notarized signature, an electronic stamp must be appended after the QES is created, as mandated by Section 23, Paragraph 1, Letter (b) of the e-Government Act. Consequently, an electronic document bearing an electronic stamp applied before the creation of a QES would be considered equivalent to a notarized signature in private law but not in public law matters.

This inconsistency in regulatory requirements for public and private law raises concerns. There appears to be no justifiable rationale for the existence of two distinct regulatory frameworks governing electronic signatures with the effect of notarized signatures in public and private law contexts. A harmonized legal approach would enhance clarity, reduce ambiguity, and ensure consistent application of electronic signature regulations across different legal domains.

4.7. Advanced and simple electronic signatures

While public law acknowledges the use of Advanced Electronic Signatures (AdES) in certain e-government services, Slovak private law does not formally recognize either AdES or Simple Electronic Signatures (SES). The acceptance of SES as a valid means of expressing intent has primarily been established through judicial decisions. However, to our knowledge, there is no judicial ruling that has explicitly addressed a private law dispute involving AdES.

As previously noted, SES is the most widely used form of electronic signature, commonly employed in various contexts, ranging from click-wrap and scroll-wrap agreements in e-commerce to emails and messaging applications. Nevertheless, Slovak courts initially encountered difficulties in recognizing declarations of intent signed using SES as legally valid. Instead, they required that all electronic declarations of intent be signed with a Qualified Electronic Signature (QES); otherwise, such declarations would be deemed invalid..

For example, the Regional Court in Žilina, in its judgment file no. 8Co/184/2018, declared the loan agreement concluded via internet banking invalid, because: *"To comply with the written form requirement, the agreement must be signed by the contracting parties in accordance with Section 40(4) of the Civil Code. However, the submitted loan agreement does not contain the defendant's handwritten signature nor a qualified electronic signature (an IP address is an identifier of a computer but not a qualified electronic signature). According to the Electronic*

Signature Act, a legal act is considered to be in written form if an act performed by electronic means is signed with a qualified electronic signature. A written statement must also be signed, meaning it becomes valid only after being signed by the acting party. A contract that is required to be in writing but has not been signed by its participants cannot produce the intended legal effects."

In contrast with this decision stands judgment file no. 6Co/30/2013 of Regional Court in Trenčín which stated that *"The absence of a qualified electronic signature in the case of an electronic legal act is not a reason for its invalidity. The validity of the contract is not contingent upon the presence of a qualified electronic signature. ... A travel arrangement contract can be validly concluded by sending an order in electronic form, which is then confirmed and delivered to the ordering party."*

Even the Supreme Court of the Slovak Republic, in its ruling file no. 2 Sžo 505/2009, in relation to the validity of a simple electronic signature, stated: *"Under the term 'electronic signature,' in addition to its statutory definition (§ 3, § 4 of Act No. 215/2002 Coll.), it is necessary to include forms of electronic signatures that are not explicitly defined by law, such as the simple inclusion of the sender's name and surname at the end of an email communication, a signature template automatically attached to an outgoing email, or any other marks or identifiers that contracting or other parties consider an identification code, by which they are able to identify the sender. These types of electronic signatures must be regarded as electronic signatures within the meaning of this term. Although a 'simple' electronic signature cannot be denied legal effect under the Directive, anyone wishing to use it for legal acts would have to prove that the requirements under § 40(3) and (4) of the Civil Code are met."*

On the European level, there are two judgments of The European Court of Justice (ECJ) which acknowledge the validity of click wrap contracts signed by SES.

First was the case of Majdoub v. CarsOnTheWeb in which ECJ concluded *"that the method of accepting the general terms and conditions of a contract for sale by 'click-wrapping', such as that at issue in the main proceedings, concluded by electronic means, which contains an agreement conferring jurisdiction, constitutes a communication by electronic means which provides a durable record of the agreement, within the meaning of that provision, where that method makes it possible to print and save the text of those terms and conditions before the conclusion of the contract".*²²

²²Judgment of the Court of Justice of 21 May 2015, Majdoub v. Cars On The Web., Deutschland GmbH. (C-322/14), EU:C:2015:236

The most recent judgment is the decision in the case of Cobult UG v. TAP Air Portugal SA from 2024 in which ECJ considered whether a passenger can validly conclude a signed agreement for reimbursement through a form available on the website of the operating air carrier. The ECJ declared that *"in the event of cancellation of a flight by the operating air carrier, the passenger is deemed to have given his or her 'signed agreement' to reimbursement of the cost of the ticket by a travel voucher where he or she has filled in an online form on the website of that air carrier, by which he or she chose such a means of reimbursement to the exclusion of reimbursement by a sum of money, where that passenger has been able to make an effective and informed choice and, accordingly, to give informed consent to the reimbursement of the cost of his or her ticket by a travel voucher rather than by a sum of money, which presupposes that that air carrier has provided to that passenger, in a fair manner, clear and full information as to the various means of reimbursement available to him or her."*²³

Despite the absence of explicit regulation in the Slovak Civil Code, the cited judicial decisions demonstrate that Simple Electronic Signatures (SES) are recognized as a valid form of electronic signature in both consumer and commercial contracts. Furthermore, we argue that the presumption established in Section 40, Paragraph 3 of the Civil Code—whereby a legal act performed electronically retains its written form if signed with a Qualified Electronic Signature (QES) should likewise extend to both Advanced Electronic Signatures (AdES) and SES.

5. WHEN PUBLIC MEETS PRIVATE

Slovak public services have been modeled after the United Kingdom's e-government framework.²⁴ As a result, these services are structured around thematic "Topics", each representing a distinct domain in which state-provided services are required. These topics comprehensively encompass various aspects of public administration, including business registration, vehicle ownership, taxation, and social services. The transition to digitalization has not altered the substantive nature of these services; rather, it has transformed traditionally paper-based processes into digital formats. Notably, the Slovak e-government portal,

²³Judgment of the Court of Justice of 21 March 2024, Cobult UG v TAP Air Portugal SA (C-76/23), EU:C:2024: 3137

²⁴ Minutes from the K9.5 Better services working group of the Ministry of Investment, Regional Development and Informatization of the Slovak Republic, 11. November 2019 session, <https://platforma.slovensko.digital/t/mirri-pracovna-skupina-k9-5-lepsie-sluzby-dizajn-manual/3160/76>, 17 February, 2025.

slovensko.sk, historically did not facilitate private transactions. However, this restriction was lifted during the COVID-19 pandemic, marking a significant shift in its operational scope.

5.1. Subsidies that broke the camel's back

During the COVID-19 pandemic, the Slovak government implemented various subsidy schemes to support businesses and individuals affected by lockdown measures. One such scheme provided financial assistance to commercial tenants who were forced to close their establishments due to government restrictions. Under this program, eligible tenants could apply for a subsidy covering up to 50% of their rent for the period during which their leased premises were subject to restricted use. However, a key condition for accessing this subsidy was the requirement for tenants to enter into a specific agreement with their landlords, wherein the landlords would agree to provide a rent discount. The government would then match the amount of the discount granted by the landlord in the form of a subsidy to the tenant.²⁵

To facilitate this process, the government introduced a standardized contract form integrated into slovensko.sk, the national electronic public services portal. Once the form was completed, both the landlord and the tenant were required to use their electronic mailboxes and Qualified Electronic Signatures (QES) to sign the agreement and submit it to the relevant ministry. This marked a significant development in Slovak e-government services, as it was the first instance in which a purely private contractual arrangement was allowed to be formalized and processed through the state's digital public services infrastructure.

Despite the scheme's successful implementation, a critical legal question remains unresolved: under which legal framework was this special contract between landlords and tenants established? The electronic completion and mutual authorization of the form effectively functioned as an agreement concerning rent discounts and the waiver of subsidy payments in favor of landlords. However, it remains unclear whether this contractual arrangement was electronically signed under civil law, given that the process followed the same procedural framework as standard public service requests. This ambiguity raises important considerations regarding the intersection of public services and private contractual relationships in the context of digital governance.

²⁵O dotácienanájomnéužmôžužiadaťpodnikateliazasiahnúťdruhouvlnoupandémie, Ministry of Economy of the Slovak Republic, <https://www.mhsr.sk/top/o-dotacie-na-najomne-uz-mozu-ziadat-podnikatelia-zasiahnuti-druhou-vlnou-pandemie>, 17 February, 2025.

5.2. Public law likes (a) company

The most recent instance of integrating private legal matters into the Slovak e-government services portal is the ability of founders of a limited liability company (LLC) to electronically conclude the company's articles of association.

Since February 2023, an amendment to Act No. 513/1991 Coll. Commercial Code (hereinafter: Commercial Code) Article 110a) and Act No. 530/2003 Coll. on the Commercial Register (Article 7a) has enabled the establishment of an LLC through a simplified electronic process. This process streamlines company formation by providing founding partners with an electronic form that includes predefined options. However, this method imposes certain limitations: the LLC may have no more than five founding partners, it can select only 15 business activities from a predefined list, and the founding partners must act personally, as representation by a proxy is not permitted. Additionally, each founding partner must possess a Qualified Electronic Signature (QES) to sign the electronic form and the articles of association.

Compared to the traditional process of establishing an LLC, this simplified approach offers two key advantages. First, it grants greater flexibility to founding partners, allowing them to form a company at any time and, theoretically, from anywhere in the world. Second, it replaces the requirement for notarized signatures on the articles of association with the use of QES, thereby eliminating the need for in-person authentication.

Despite these undeniable benefits, the introduction of this electronic procedure raises a legal question similar to the one encountered in the subsidy scheme. In the traditional paper-based process, the signatures of founding partners must be notarized. As previously noted, there are distinct legal frameworks governing the equivalence of a notarized signature in electronic legal acts under public and private law. This leads to a fundamental legal uncertainty: which legal framework governs the conclusion of a private contract²⁶ executed on a public digital platform? At present, neither the Slovak e-Government Act nor the Civil or Commercial Code provides a definitive answer to this question.

²⁶ Smejkal, V., et al., *Právoinformačních a telekomunikačních systémů*. 2. vyd. Praha : C. H. Beck, 2004. p. 343.

5.3. Electronic public services in commercial activities

Access to public services provides certain businesses with a significant advantage. One of the most sought-after public services is the Register of Residents, managed by the Ministry of the Interior. This register consolidates personal data of Slovak citizens and foreign nationals residing in Slovakia, including their residency information.²⁷ Access to this database enables businesses to verify the identity of their clients efficiently. However, such access has been exclusively granted to banks.

For instance, Tatrabanka, one of Slovakia's major financial institutions, claims that access to the Register of Residents has saved significant time for approximately 60,000 clients.²⁸ Customers no longer need to visit a physical branch to update their residency or other personal details, as the bank's internal records are automatically synchronized with the register whenever a change occurs. This privileged access was granted through an amendment to the Act No. 483/2001 Coll. Banking Act (hereinafter: Banking Act), which enabled the conclusion of electronic communication agreements between banks and public institutions via a dedicated information system. According to Section 90, Paragraph 3 of The Banking Act, this system must ensure "*smooth, reliable, and secure information exchange.*"

At present, banks remain the only private entities permitted to access public registers. Attorneys, notaries, and other businesses subject to anti-money laundering (AML) regulations are excluded from such access, despite their legal obligations to perform due diligence. While the protection of personal data against unauthorized access and potential breaches is a legitimate concern, the current legal framework fails to reconcile data protection with the practical need for businesses to access relevant public registers in order to comply with AML requirements.

²⁷Register obyvateľov SR, Ministry of Interior of the Slovak Republic, <https://www.minv.sk/?register-obyvatelov-sr>, 20 February, 2025.

²⁸Miklošovičová, S.: Ušetrímečas 60-tisíc klientomročne, Press release, 26. 04. 2023, <https://www.tatrabanka.sk/sk/blog/tlacove-spravy/usetime-cas-60-000-klientov-rocne/>, 20 February, 2025.

5.4. The tale of two e-wallets

The European Digital Identity Framework²⁹, which entered into force in May 2024 and amended the eIDAS regulation, has introduced an EU Digital Identity Wallet (EUDI Wallet) is to allow *"the user to securely store, manage and validate personal identification data and electronic attestations of attributes for the purpose of providing them to relying parties and other users of European Digital Identity Wallets, and to sign by means of qualified electronic signatures or to seal by means of qualified electronic seals"* (Article 3 (42) of eIDAS Regulation). EUDI Wallet is expected to be publicly released by 2026.

The European Commission lists several advantages of EUDI Wallets, such as: identifying a payer of transaction, identification to open bank accounts without visiting a branch, storing professional qualifications, claiming prescriptions, accessing social security benefits, SIM registration, identification for the purposes of travel and booking, signing contracts, as a proof that a person is a legitimate representative of an organization, storing mobile driving license.³⁰

In anticipation of of EUDI Wallets, Slovakia has amended the Trust Services Act (Sections 10 and 11) to align with the new European framework. This legislation designates the Ministry of the Interior as the official provider of EUDI Wallets on behalf of the state (Article 5a (2), paragraph (a) of the eIDAS Regulation) and establishes procedures for issuing and revoking wallets based on the requirements for a qualified trust service.

However, Slovakia is also developing its own national e-wallet, an electronic alternative to physical identity cards and driving licenses, set to launch between February and March 2025.³¹ The legal framework for this initiative is defined by Act No. 364/2024 Coll., which amends Act No. 8/2009 Coll. on Road Traffic. According to this legislation, data stored in the national e-wallet can only be verified using a dedicated mobile verification application managed by the Ministry of the Interior, and only law enforcement authorities are authorized to accept this digital identity as a legally binding alternative to physical documents.

²⁹ 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, OJ L, 2024/1183, 30.4.2024

³⁰Why EU Digital Identity Wallets, European Commission, <https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/Benefits>, 20 February, 2025.

³¹Minútapominúte, 30. December 2024 11:49, Denník N, N Press, s.r.o., <https://dennikn.sk/minuta/4383371/>, 20 February, 2025.

A critical uncertainty remains: Will Slovakia's national e-wallet be integrated into the EUDI Wallet, or will it operate as a standalone system? The coexistence of these two parallel digital identity solutions appears redundant and may create confusion among users. If the national e-wallet remains a separate initiative with limited use cases, its long-term viability is questionable.

5.5. The Great Hack

At the time of writing, public trust in Slovak electronic public services has suffered a severe setback due to a major cybersecurity breach. On January 5, 2025, at 8:50 AM, the Geodesy, Cartography, and Cadastre Office of the Slovak Republic fell victim to a ransomware attack, which encrypted all cadastral data, rendering real estate ownership records and associated services inaccessible.³²

In the immediate aftermath, the Ministry of the Interior downplayed the severity of the incident. In a press release, the ministry initially stated:

*"Due to the necessary adjustments to the information systems managed by the Geodesy, Cartography, and Cadastre Office of the Slovak Republic, the cadastral departments of the district offices will not provide services on Tuesday, January 7, 2025, and will offer services in a limited capacity on the following days as well".*³³

Despite assurances from the Cadastre Office and the Ministry of the Interior that recent backups existed³⁴, the reality has been far more troubling. More than 50 days after the attack, electronic cadastre services have not yet been fully restored, and operations remain reliant on a limited backup system.

This cyberattack is the most severe in Slovakia's history, with wide-ranging repercussions: real estate transactions have been delayed or frozen, creating uncertainty in the property market; property tax collection has been disrupted, potentially affecting municipal revenues; insurance companies have struggled to verify property ownership for policy underwriting and claims processing; the

³²Trangel, J., Všetko o hackerskom útoku na kataster: Prehľadné otázky a odpovede, Ringier Slovakia Media s.r.o., 9.1.2025, <https://zive.aktuality.sk/clanok/D0efBvf/vsetko-o-hackerskom-utoku-na-kataster-prehladne-otazky-a-odpovede/>, 23 February, 2025.

³³Združeniemiest a obcí Slovenska: Katastrálneodboryokresnýchúradovbudú v nasledovnýchdňochposkytovaťslužby v obmedzenomrežime, 6.1.2025, <https://www.zmos.sk/katastralne-odbory-okresnych-uradov-budu-v-nasledovnych-dnoch-poskytovat-služby-v-obmedzenom-rezime-oznam/mid/536833/.html/>, 23 February, 2025.

³⁴TA3: Katastermäšťrizálohy, hekerižiadali 12 miliónovdolarov, tvrdíHorecký. Niktoneviepovedať, kedysaznovarozbehne, 14.1.2025, <https://www.ta3.com/clanok/975725/kataster-ma-styri-zalohy-hekeri-ziadali-12-milionov-dolarov-tvrdi-horecky-nikto-nevie-povedat-kedy-sa-znova-rozbehne>, 23 February, 2025.

construction sector has faced delays due to difficulties in obtaining necessary land registry data.

Beyond its economic and administrative impact, the attack has also had a profound psychological effect. Public trust in governmental competence and the security of electronic data has been significantly eroded.³⁵ The incident has also become a subject of widespread online ridicule, with social media users creating memes mocking the government's response.³⁶

Perhaps most concerning is how the attack has exposed the vulnerability of Slovakia's digital infrastructure. It has also highlighted a broader political issue: the reluctance of officials to engage in transparent communication with the public. Rather than acknowledging the full scope of the crisis, authorities appear to have prioritized damage control and political optics over accountability.³⁷

6. CONCLUSION

The digitalization of public and private services in Slovakia has revealed significant discrepancies in legal frameworks, technological implementation, and user adoption. While private digital services, particularly e-commerce, have flourished, public e-government services have struggled to achieve similar levels of accessibility and efficiency. This divergence is partially attributable to inconsistencies in legal regulation, such as the contradictory treatment of electronic signatures and seals under national and EU law, as well as the rigid and sometimes impractical requirements for qualified electronic signatures in public services.

The Slovak government's approach to digital identification, particularly through electronic IDs and mandate certificates, has proven to be both restrictive and administratively burdensome, limiting user engagement and stifling potential innovation. While recent allowances for advanced electronic signatures (AdES) in

³⁵Haluza, I., Kolaps katastra ohrozuje dôveru. Predávať byty a pôdu možno budeme zase iba s pečiatkou z úradu, hovorí farmár, Denník N, N Press, s.r.o., 15. January 2025, <https://e.dennikn.sk/4406012/kolaps-katastra-ohrozuje-doveru-predavat-byty-a-podu-mozno-budeme-zase-iba-s-peciattkou-z-uradu-hovori-farmar/>, 23 February, 2025.

³⁶ See Facebook posts from ZOMRI on January 14, January 23, February 5 2025.

³⁷Burčák, M., Päťdnízahmlievania a päťhlavnýchmomentov. Pádkatastraštatnézvládolvysvetliť, SME.sk, Petit Press, a.s.,10. January 2025, <https://domov.sme.sk/c/23434070/kataster-pad-vlada-komunikacia.html>, 23 February, 2025.

certain public services indicate a step toward flexibility, the lack of transparency and clarity regarding their implementation diminishes their practical effectiveness. Furthermore, the reluctance to integrate private sector solutions into public digital services, as exemplified by the limited access of businesses to essential public registers, further constrains the development of a more integrated and efficient digital ecosystem.

Moreover, recent security failures, such as the catastrophic ransomware attack on the Cadaster Office, highlight the urgent need for more robust cybersecurity measures and crisis management strategies. The erosion of public trust resulting from this incident underscores the importance of not only implementing secure digital infrastructure but also fostering transparent communication and proactive policymaking.

This paper contributes both scientifically and professionally to the evolving discourse on the intersection of law and digital services, particularly within the Slovak context. From an academic standpoint, this paper provides a foundational analysis of how Slovak private and public law are evolving or encountering challenges in response to the demands of an increasingly digitalized society. In the realm of private law, it highlights how Slovak jurisprudence has cautiously recognized electronic contracts as equivalent to traditional written or oral agreements. In the domain of public law, it emphasizes that fostering greater flexibility, transparent communication, and predictability could enhance public trust in e-government services.

On a professional level, this paper aims to provide actionable insights for legal professionals, policymakers, and digital service providers engaged with Slovakia. It identifies legislative and administrative deficiencies that impede the effective integration of digital services and advocates for the adoption of European-level solutions over national approaches. Such harmonization has the potential to significantly enhance the uptake of public services on unified platforms, encompassing both public and private sectors. Furthermore, facilitating secure business access to electronic public databases could inadvertently foster greater utilization of public services.

Ultimately, the Slovak experience serves as a case study of the broader challenges faced by governments attempting to balance security, accessibility, and legal compliance in digital services. Addressing these issues requires a more harmonized approach to legal frameworks and a user-centered focus that prioritizes both security and convenience. Without such measures, Slovakia risks falling further behind in its digital transformation, both in the public and private spheres.

REFERENCES

BOOKS AND ARTICLES

1. Smejkal, V., et al.: Právoinformačních a telekomunikačních systémů. 2. vyd. Praha : C. H. Beck, 2004.
2. Števček, M., Dulak, A., Bajánková, J., Fečík, M., Sedlačko, F., Tomašovič, M. a kol. Občiansky zákonník II. 2. vydání. Praha: C. H. Beck, 2019, marg. č. 10.
3. Treščáková, D.: Právoelektronického obchodu, Širšie súvislosti. Praha: Leges, 2021.

LEGAL ACTS

1. Act No. 272/2016 Coll. on Trust Services for Electronic Transactions in the Internal Market
2. Act No. 305/2013 Coll. on the electronic execution of public authority powers
3. Act No. 364/2024 Coll., which amends Act No. 8/2009 Coll. on Road Traffic
4. Act No. 483/2001 Coll. Banking Act
5. Act No. 513/1991 Coll. Commercial Code
6. Act No. 530/2003 Coll. on the Commercial Register
7. Civil Code Act No. 40/1964 Coll.
8. Decree No. 511/2022 Coll. of the Ministry of Investments, Regional Development, and Informatization of the Slovak Republic on Recognized Methods of Authorization
9. Decree No. 511/2022 Coll. of the Ministry of Investments, Regional Development, and Informatization of the Slovak Republic on Recognized Methods of Authorization
10. Decree No. 70/2021 Coll. on Guaranteed Conversion
11. 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, OJ L, 2024/1183, 30.4.2024
12. 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, 28.8.2014, p. 73–114

COURT DECISIONS

1. Judgment of the Court of Justice of 21 March 2024, Cobult UG v TAP Air Portugal SA (C-76/23), EU:C:2024: 3137
2. Judgment of the Court of Justice of 21 May 2015, Majdoub v. CarsOnTheWeb., Deutschland GmbH. (C-322/14), EU:C:2015:236
3. Regional Court in Trenčín, judgment file no. 6Co/30/2013
4. Regional Court in Žilina, judgment file no. 8Co/184/2018
5. Supreme Court of the Slovak Republic, judgment file no. 2 Sžo 505/2009

NETWORK RESOURCES

1. Bezkontaktné biometrické občianske preukazy pre obyvateľov EÚ budúrealitou. Ministerstvo vnútrapripravuj eichvydávanie, SITA Slovenská tlačová agentúraa.s, 17. 11. 2022, <https://sita.sk/bezkontaktno-biometricko-obcianske-preukazy-pre-obyvatelov-eu-budu-realitou-rezort-vnutra-pripravuje-ich-vydavanie/>, 2 February, 2025.
2. Burčík, M., Páďdnízahmlievania a páďhlavnýchmomentov. Páďkatastraštátne zvládol vysvetliť, SME.sk, Petit Press, a.s., 10. January 2025, <https://domov.sme.sk/c/23434070/kataster-pad-vlada-komunikacia.html>, 23 February, 2025.
3. COVID-19: Embracing digital government during the pandemic and beyond, UN. Department of Economic and Social Affairs, April 2020, <https://digitallibrary.un.org/record/3856978?v=pdf&ln=en>, 24 January, 2025.
4. eSignature FAQ, What is the difference between an electronic signature and a digital signature? European Commision, <https://ec.europa.eu/digital-building-blocks/sites/display/DIGITAL/eSignature+FAQ>, 27 January, 2025.
5. ETSI TR 119 001 V1.2.1 (2016-03), Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations, https://www.etsi.org/deliver/etsi_tr/119000_119099/119001/01.02.01_60/tr_119001v010201p.pdf 27 January, 2025.
6. EU/EEA Trusted List Browser, eIDAS Dashboard, <https://eidas.ec.europa.eu/efda/trust-services/browse/eidas/tls>, 27 January, 2025.
7. Government Bill on the Electronic Form of the Exercise of Public Authority and on Amendments and Supplements to Certain Laws (e-Government Act), Explanatory Report – Special Part, <https://www.nrsr.sk/web/Dynamic/DocumentPreview.aspx?DocID=384288>, 2 February, 2025.

8. Haluza, I., Kolaps katastra ohrozuje dôveru. Predávať byty a pôdu možno budeme zase iba s pečiatkou z úradu, hovorí farmár, Denník N, N Press, s.r.o., 15. January 2025, <https://e.dennikn.sk/4406012/kolaps-katastra-ohrozuje-doveru-predavat-byty-a-podu-mozno-budeme-zase-iba-s-peciattkou-z-uradu-hovori-farmar/>, 23 February, 2025.
9. Kosno, L., Podpisujete sa e-občianskym starým typom? Dočasné riešenie má fungovať iba polrok, Ringier Slovakia Media s.r.o., 25.11.2022, <https://zive.aktuality.sk/clanok/zOxZBfI/podpisujete-sa-e-obcianskym-stareho-typu-docasne-riesenie-ma-fungovat-iba-polrok/>, 2 February, 2025.
10. Kosno, L., Žiadosti o nové e-občianske lámal rekordy. Štát tvrdí, že doklady doručí včas, Ringier Slovakia Media s.r.o., 18.1.2023, <https://zive.aktuality.sk/clanok/mpybc5I/ziadosti-o-nove-e-obcianske-lamali-rekordy-stat-tvrdi-ze-doklady-doruci-vcas/>, 2 February, 2025.
11. Miklošovičová, S., Ušetríme čas 60-tisíc klientom ročne, Press release, 26.04.2023, <https://www.tatrabanka.sk/sk/blog/tlacove-spravy/usetrim-cas-60-000-klientov-rocne/>, 20 February, 2025.
12. Minúta pominúte, 30. December 2024 11:49, Denník N, N Press, s.r.o., <https://dennikn.sk/minuta/4383371/>, 20 February, 2025.
13. Minutes from the K9.5 Better services working group of the Ministry of Investment, Regional Development and Informatization of the Slovak Republic, 11. November 2019 session, <https://platforma.slovensko.digital/t/mirri-pracovna-skupina-k9-5-lepsie-sluzby-dizajn-manual/3160/76>, 17 February, 2025.
14. Dotácie na najomné už môžu žiadať podnikatelia zasiahnutí druhou vlnou pandémie, Ministry of Economy of the Slovak Republic, <https://www.mhsr.sk/top/o-dotacie-na-najomne-uz-mozu-ziadat-podnikatelia-zasiahnuti-druhou-vlnou-pandemie>, 17 February, 2025.
15. Platnosť certifikátu pre vydávanie e-podpisu a občianskych preukazov a cudzineckých dokladov končí 26. júna, používať vydané certifikáty však budeme ešte až do konca roku 2022, Ministry of Interior of the Slovak Republic, 26. 05. 2021 Press Release, <https://www.minv.sk/?tlacove-spravy&sprava=platnost-certifikatu-pre-vydavanie-e-podpisu-na-obcianskych-preukazoch-a-cudzineckych-dokladoch-konci-26-juna-pouzivat-vydane-certifikaty-vsak-bude-mozne-az-do-konca-roku-2022>, 2 February, 2025.
16. Predĺženie používania uznaného spôsobu autorizácie, National Agency for Network and Electronic Services, 06. 11. 2024, https://www.slovensko.sk/sk/oznamy/detail/_predlzenie-pouzivania-uznaneho, 2 February, 2025.
17. Prehľad vydávania elektronických občianskych preukazov a certifikátov pre vytvorenie kvalifikovaného elektronického podpisu (eID štatistika) k 31.12.2024

- (PDF, 200 kB),
https://www.minv.sk/swift_data/source/policia/md_ode/eid_statistika/2024_eid_statistika/eID%20statistika_12.pdf, 30 January. 2025.
18. Qualified Signature/Seal Creation Devices and Secure Signature Creation Devices, European Commission, eIDAS Dashboard, <https://eidas.ec.europa.eu/efda/browse/notification/qscd-sscd>, 27 January, 2025.
 19. Register obyvateľov SR, Ministry of Interior of the Slovak Republic, <https://www.minv.sk/?register-obyvatelov-sr>, 20 February, 2025.
 20. Roseth, B.; Reyes, A.; Yee Amézaga, K., Public Services and Digital Government during the Pandemic: Perspectives of Citizens, Civil Servants, and Government Institutions, Inter-American Development Bank., 2021, <http://dx.doi.org/10.18235/0003122>, 24 January, 2025.
 21. See Facebook posts from ZOMRI on January 14, January 23, February 5, 2025.
 22. TA3: Kataster máštyrizálohy, hekerižiadali 12 miliónov dolárov, tvrdí Horecký. Niktonevie povedať, kedysaznovarozbehne, 14.1.2025, <https://www.ta3.com/clanok/975725/kataster-ma-styri-zalohy-hekeri-ziadali-12-milionov-dolarov-tvrdi-horecky-nikto-nevie-povedat-kedy-sa-znova-rozbehne>, 23 February, 2025.
 23. Tomek, R., Graf dňa: Rozširovanie Governmentu s avlanina Slovenska v jedinej krajine regiónu zastavilo, Denník N, N Press, s.r.o., 16. February 2022, <https://e.dennikn.sk/2724194/graf-dna-slovensko-sa-v-elektronickej-komunikacii-so-statom-prepadlo-pod-priemer-eu/>, 24 January, 2025.
 24. Trangel, J., Všetko o hackerskom útoku na kataster: Prehľadné otázky a odpovede, Ringier Slovakia Media s.r.o., 9.1.2025, <https://zive.aktuality.sk/clanok/D0efBvf/vsetko-o-hackerskom-utoku-na-kataster-prehladne-otazky-a-odpovede/>, 23 February, 2025.
 25. Vyhláška o uznaných spôsoboch autorizácie a nasadení zmeny, National Agency for Network and Electronic Services, <https://www.slovensko.sk/sk/institucie-formulare-a-ziado/vyhlasaka-o-uznanych-sposoboch>, 2 February, 2025.
 26. Vyhláška o uznaných spôsoboch autorizácie a zoznam služieb, National Agency for Network and Electronic Services, 30. 12. 2022, https://www.slovensko.sk/_img/CMS4/Zoznam_sluzieb_USA.xlsx, 2 February, 2025.
 27. Vyhláška o uznaných spôsoboch autorizácie a zoznam služieb, National Agency for Network and Electronic Services, 30. 12. 2022, https://www.slovensko.sk/sk/oznamy/detail/_vyhlaska-o-uznanych-sposoboch, 2 February, 2025.
 28. Why EU Digital Identity Wallets, European Commission, <https://ec.europa.eu/digital-building->

- blocks/sites/display/EUDIGITALIDENTITYWALLET/Benefits, 20
February, 2025.
29. Združením miest a obcí Slovenska: Katastrálne odbory okresných úradov budú v
nasledovný ch dňoch poskytovať služby v obmedzenom režime, 6.1.2025,
<https://www.zmos.sk/katastralne-odbory-okresnych-uradov-budu-v-nasledovnych-dnoch-poskytovat-sluzby-v-obmedzenom-rezime-oznam/mid/536833/.html>, 23 February, 2025.