Bratislava International School of Liberal Arts

A Utopia for Realists: Effective e-Government in Slovakia

BACHELOR THESIS

Bratislava, 2023 Lucia Kobzová

Bratislava International School of Liberal Arts

A Utopia for Realists: Effective e-Government in Slovakia

BACHELOR THESIS

Study Program: Liberal Arts
Field of Study: 6718 Political Science
University: Bratislava International School of Liberal Arts
Thesis Supervisor: Mgr. Dagmar Kusá, PhD.
Degree of Qualification: Bachelor of Arts (BA)
Date of Submission: February 15, 2023
Date of Defence: June 12, 2023

Bratislava, 2023 **Lucia Kobzová**

Declaration of Originality

I hereby declare that this bachelor´s thesis is my own work and has not been published in part or in whole elsewhere. All used literature and other sources are attributed and cited in References.

In Bratislava, 15 February 2023 **Lucia Kobzová**

Abstract

Author: Lucia Kobzová
Title: A Utopia for Realists: Effective e-Government in Slovakia
University: Bratislava International School of Liberal Arts
Thesis Supervisor: Dagmar Kusá, PhD.
Date of Submission: February 15, 2023
Date of Defence: June 12, 2023
Chair of the Defence Committee: prof. PhDr. František Novosád, CSc.
Thesis Defence Committee: Prof. PhDr. František Novosád, CSc., doc. Samuel Abrahám, PhD., Mgr. Dagmar Kusá, PhD., prof. Silvia Miháliková

Key terms: e-government, Slovakia, legal framework, public e-services, cybersecurity

This research is devoted to examining the elements that are *sine qua non* for the effective functioning of e-governance in Slovakia. Even though myriad factors impact the electronic exercise of public authority, the data reveals that the predominant emphasis ought to be given to three major aspects that determine the success of e-governance**.** First, the legal framework should emanate from deeper comprehension of technological solutions and ensure data security. Second, proposed e-policies must comply with the highest cyber security standards. Last but not least, there should be high-quality online public services that are proactive. The aim is to evaluate the overall functioning of e-government in Slovakia. Although various studies examine specific aspects of e-government in Slovakia, more complex research that would evaluate different elements of effective e-government seem to be missing.

This paper underlines the obstacles and deficits that hinder the effective functioning of e-government in Slovakia. Even though it was anticipated that the legal framework would pose a major obstruction in the effective functioning of Slovak e-government, the most significant obstacle is public e-services. Public e-services need to be more proactive and of high quality and scope. Cybersecurity measures are considered efficient, except for almost absent education measures. The thesis concludes that Slovak e-government is functional while policymakers should focus on public e-services, regulation level of the legal framework, and cybersecurity education measures.

Abstrakt

Autorka: Lucia Kobzová
Názov: Utópia pre Realistov: Efektívny e-Government na Slovensku
Univerzita: Bratislavská Medzinárodná Škola Liberálnych Štúdií
Školiteľka bakalárskej práce: Dagmar Kusá, PhD.
Dátum odovzdania bakalárskej práce: 15 február, 2023
Dátum obhajoby bakalárskej práce: 12 jún, 2023
Predseda komisie pre obhajobu bakalárskej práce: prof. PhDr. František Novosád, CSc.
Komisia pre obhajobu bakalárskej práce: Prof. PhDr. František Novosád, CSc., doc. Samuel Abrahám, PhD., Mgr. Dagmar Kusá, PhD., prof. Silvia Miháliková

Kľúčové slová: e-government, Slovensko, právny rámec, verejné e-služby, kyberbezpečnosť

Tento výskum je venovaný skúmaniu elementov, ktoré sú *sine qua non* pre efektívne fungovanie e-governmnetu na Slovensku. Hoci na elektronický výkon verejnej moci vplýva množstvo faktorov, dáta ukazujú, že je potrebné klásť dôraz na tri hlavné aspekty určujúce úspech e-governmentu. Právny rámec musí vychádzať z hlbšieho pochopenia technologických riešení a musí garantovať bezpečnosť údajov. Navrhované e-politiky musia taktiež spĺňať najvyššie štandardy v oblasti kyberbezpečnosti. V neposlednom rade by mal štát poskytovať kvalitné a proaktívne online služby. Cieľom je zhodnotiť celkové fungovanie e-governmentu na Slovensku. Existujú rôzne štúdie skúmajúce konkrétne aspekty e-governmentu na Slovensku, chýba však komplexnejší výskum hodnotiaci rôzne prvky efektívneho elektronického výkonu verejnej moci.

Táto práca poukazuje na prekážky a deficity brániace efektívnemu fungovaniu e-governmentu na Slovensku. Predpokladalo sa, že právny rámec bude predstavovať najväčšiu prekážku. Napokon sa však ukázalo, že najväčším úskalím sú verejné e-služby. Elektronické služby musia byť proaktívnejšie a mať vyššiu kvalitu a rozsah. Opatrenia v oblasti kybernetickej bezpečnosti možno považovať za efektívne s výnimkou nedostatočných vzdelávacích opatrení. Záverom práce je zhodnotenie, že slovenský e-government je fungujúci pričom by sa mali tvorcovia politík zamerať na e-služby, úroveň regulácie zákonov a vzdelávacie opatrenia v oblasti kybernetickej bezpečnosti.

Acknowledgements

I would like to express my appreciation to my advisor Mgr. Dagmar Kusá, PhD. for her support, guidance, and valuable advice. I would like to also thank Ministry of Investments, Regional Development, and Informatization for giving me an opportunity to intern at the section of information technologies of public administration. This experience gave me knowledge that helped me to conduct this research. I want to express my gratitude to my family and friends for their endless support during my studies and while writing this thesis.

Vocabulary

Blockchain - database for storing electronic data. Blockchain stores information in blocks that cannot be changed which is the reason for its considerable level of security. This solution is used when it is desirable not to modify data (e.g. transactions or health data about patients).

Digitization – the process of converting information from the physical world to its digital representation.

Digitalization – the process of utilizing digital technologies to enable and improve procedures within a specific environment.

G2G communication - abbreviation of government-to-government communication. It refers to interactions between governmental institutions on a national level. The form of interaction is unspecified, while the emphasis is given to its existence.

G2C communication - abbreviation of government-to-citizens communication. It refers to interactions between the government and citizens. The form of interaction is unspecified, while the emphasis is given to its existence.

G2B communication - abbreviation of government-to-business communication. It refers to interactions between government and private sector entities. The form of interaction is unspecified, while the emphasis is given to its existence.

Interoperability of databases – the ability of various database systems to connect and exchange data without restrictions. In terms of e-government, it refers to the fact that databases should automatically exchange information when a citizen needs public service.

Law in action – legal doctrine according to which laws are interpreted as they are used in practice. Legal texts tend to differ from their application in practice, so legal scholars compare the legal practice to legal texts.

Law in books – legal doctrine according to which laws are interpreted as written, not as they are used in practice.

Once only – approach according to which citizens, institutions and companies should not give the government the same information more than once. When specific information about the user enters the governmental information system, the state should internally share this information instead of asking the user to enter it again.

Security by design – an approach to cybersecurity that requires the implementation of preventive measures before implementing a specific project or solution.

Table of content

List of figures

1. Slovakia and its Struggle with Digitalization

I grew up in a family of accountants. My mother, cousin and godmother own a small accounting firm. I have many memories from my childhood when I had to visit with them various state institutions regularly to file documents that were required by the law. I remember sometimes standing for hours in long queues when the deadlines were approaching. I also remember the initial joy after the government introduced digital services that facilitated communication with the state authorities. However, it was not a smooth transition, but various flaws accompanied the journey of e-services. The initial interface was far from being user-friendly; when many accountants wished to upload documents, the system either slowed down enormously or entirely collapsed, and users would get contradictory messages from different institutions about (un)successful upload of a document. Even though the e-services used by accountants have incredibly improved over the years, other information systems used by citizens for communication with the state authorities remain inefficient. This experience is a vivid example of how well-established state online services could positively impact individuals' lives.

The world has dramatically changed over the past few decades. As a result of the interconnectedness of the physical and digital world, we can no longer separate the things that happen online from those that happen offline and vice versa. Digitalization has not only affected our social life as a prevailing number of our interactions take place in the digital realm. More importantly, technologies shifted the conduct of politics. Vis-á-vis digital transformation, governments are forced to respond to diverse hybrid threats, including cyber-attacks, disinformation strategies, or even cyber espionage. Furthermore, if a state is to remain competitive in a digitalized world, it must, *inter alia,* undergo a process of digitization and digitalization and, at the same time, offer services to the citizen that would adequately reflect the standards of the 21st century. Therefore, the question could be raised which practices and measures a state should adopt in order to react to technological progress appropriately. In Slovakia, a state considered an integral part of the European community, the necessity to remain competitive and adjust to rapidly changing digital trends is even more evident. However, there are two major obstacles that every government in Slovakia will face when implementing digital solutions- high corruption levels and the state's extreme bureaucratic burden.

The major obstruction in implementing desirable solutions is often the high complexity of bureaucratic processes. Slovakia is well-known for its extensive bureaucratic apparatus, which precludes faster progress of the state. Even though Slovakia might never become an administrative haven as Estonia, the need for debureaucratization is indisputable. Political leaders have been attempting to resolve this issue rhetorically for over a decade. So far, without any tangible result. Public procurement, drawing the EU funds, requirements for EU projects, and citizen to government (C2G) communication are just a few examples of this negative phenomenon.

One of the possible solutions to facilitate the excessive complexity of administrative processes in C2G communication is the introduction of e-government. In Estonia, the implementation of e-solutions brought lower levels of administrative complexity. E-policies might then shift the paradigm in terms of alleviating the extreme bureaucratic burden that is imposed on citizens in Slovakia. Moreover, the lower levels of administrative requirements could help both the citizens and businesses. It would create a friendlier business environment and, at the same time, contribute to the well-being of the citizens since they could communicate with a state in a less demanding manner.

One of the most significant problems that Slovakia has been facing ever since the establishment of the Republic in 1993 is omnipresent corruption. Corruption often goes undetected since transparency of processes and acts within public administration is often neglected or even ignored. E-policies could offer a desirable solution to this problem. The primary benefit of digital policies is a greater level of transparency since every transaction or communication that occurs in digital space leaves a digital footprint that is easily traceable. Therefore, if the government decides to implement policies based on blockchain or other relevant technological solutions, corruption could be detected in a simple manner. Corruption decreases trust in institutions and undermines the legitimacy of elected government.

Reducing the corruption could then lead to improving the quality of democracy as such. Lower levels of corruption and greater transparency can result in greater trust toward institutions. For democracy to function it is necessary to have citizens who trust that institutions work independently, that they are not corrupt, and when their rights are violated, they could seek an effective remedy in a just judiciary environment. Democracy ought to be participatory. Communication with state in digital realm could alleviate the obstacle preventing people from participation in public affairs. Introducing e-government solutions could hence lead to higher quality of democracy.

Slovak legal framework does not correspond with the technological possibilities. This prevents faster progress in the digitalization of the state. Lawyers who formulate legislation for information technologies often lack sufficient knowledge of technical constraints and vice versa- developers de facto disregard the necessity to have an adequate legal framework for proposed e-solutions. Besides, the security concerns that might be addressed in the digital world could conflict with the human rights of citizens and the legislature in general. Therefore, it seems more than relevant to focus on the amalgamation of the legal framework and technological measures and offer a comprehensive overview of attributes on which effective e-government should be built.

1.1 Through Digitalization to Strengthening Democracy

Experts agree that digitalisation is an ambivalent phenomenon since, on the one hand, it has the potential to enhance democratic processes by increasing accountability and openness of the government. On the other hand, it facilitates the misuse of personal information and could infringe on the right to privacy (Adams & Prins, 2017). E-governance could have various beneficial effects, *inter alia,* corruption reduction, the inclusion of minorities, participation of excluded people, investment attraction, better public services, greater transparency, and cost reduction (Metcalf, 2014; Shim & Eom, 2008; Adams & Prins, 2017; Twizeyimana & Andersson, 2019). As Metcalf (2019) states, e-government solutions are not detrimental or beneficial per se, but the manner in which they are used is essential for determining their added value. The crucial elements that distinguish effective e-governance from simple electronic solutions of the state are interactivity and interoperability (Metcalf, 2019). Interactivity describes the possibility of interacting with the state in digital space. Interoperability refers to the interconnectedness of databases which facilitates the exchange of information and hence creates a coherent system for e-services (Metcalf, 2019). Another attribute of effective e-governance identified in the study is a coherent system for services offered to the users (Metcalf, 2019). Estonia could serve as an example of this model since all electronic services are available on one website(eesti.ee), so the users do not have to search through various platforms, but everything can be found on this web portal (Metcalf, 2019). In addition, creating a governing body that would cover the whole e-government agenda would be desirable for enhancing the effectiveness of digital services (Metcalf, 2019). However, many remain sceptical towards technological solutions since there is a concern that they might lead to enhanced levels of surveillance, deepening inequalities, or even infringements concerning personal data (Metcalf, 2019; Adams & Prins, 2017).

There is no need to propose a fundamentally different legal system for e-governance, but there are undeniable differences between the physical and digital worlds. For that reason, the legislature must be designed in a manner that would correspond with technological requirements (Metcalf, 2014). According to Metcalf (2019), it is not desirable to regulate e-governance legally to a great extent, but the law should be rather facilitative for e-solutions.

It emanates from the fact that over-regulation might preclude innovation, and hence a greater level of flexibility is required. However, the legal framework must precisely cover specific areas. Regulatory laws should be introduced to specify the conditions necessary for e-identification, e-signature, and data privacy. Therefore, it is suggested that there should be two possible functions of the laws regarding e-governance- facilitative and regulatory (Metcalf, 2014).

The primary focus of proposed policies should be given to security since citizens will only accept e-solutions that are deemed reliable and secure (Metcalf, 2014). Furthermore, there is an increased potential for political misuse of information the state possesses about citizens since the data are only one click away (Dutt & Karikmäe, 2014). Therefore, the crucial part of functional digital policies is focusing on well-defined data protection laws. This is necessary not only for a comprehensive and coherent legal framework but, more importantly, for the security of e-solutions (Metcalf, 2019). The European Union attempts to address this problem by initiating legislation concerning data protection as a complementary framework for the rights derived from the European Convention for Human Rights, which is a cornerstone of the European Charter on Fundamental Rights (Dutt & Karikmäe, 2014). The traceability of digital transactions presents both a threat and a benefit for e-governance (Dutt & Karikmäe, 2014). On the one hand, it establishes an interface where a greater level of transparency is possible, but on the other hand, it poses a threat to data privacy derived from the right to privacy (Dutt & Karikmäe, 2014). Furthermore, the design of e-solutions must be user-friendly, which often hinders respecting the principles of security in the digital realm (Metcalf, 2019). E-identification could serve as an example of this dichotomy. The identification system must be secure for all types of transactions, whilst it is necessary to design it in a manner that would be comprehensive for all entities that interact with the state (Metcalf, 2019).

Research indicates that two major aspects could positively impact the effectiveness of e-governance: 1) A well-formulated legal framework that respects technological limitations, 2) High security of digital services. The primary issue with implementing digital policies is that the proposed technological solutions do not always correspond with legal limitations. For that reason, it is desirable first to analyse the specific legal system of the state in order to avoid the failure to implement certain e-services due to legal obstacles. As several studies suggest, it could be beneficial for the states to follow the Estonian digitalization model. However, the implementation of Estonian digital solutions is, in many regards, not possible in Slovakia due to legal constraints. Major obstruction that will hinder effective e-government solutions is the trust in institutions which is extremely low in Slovakia. In addition, the comprehension of complex technical solutions amongst the population is relatively low. Due to this fact, the willingness to accept and followingly trust e-solutions will pose a major problem for the successful digitalisation of Slovakia. Therefore, the purpose of this study is to offer a well-arranged overview of three major elements that seem to have a decisive effect on the success of e-solution, with an emphasis on a well-formulated legal framework that is an absolute necessity for effective e-governance. The study points out which approaches ought to be eliminated or even eradicated if the government decides to implement digital policies and which approaches should be given greater emphasis.

The effectiveness of e-governance could be enhanced by:

A) a coherent set of laws that incorporate and reflect the technological constraints and ensure data protection and privacy;

B) cybersecurity measures that ensure digital services are resistant to current threats and vulnerabilities as well as are designed in a manner to detect and resolve cyber incidents, restore data, and minimize the possible negative consequence;

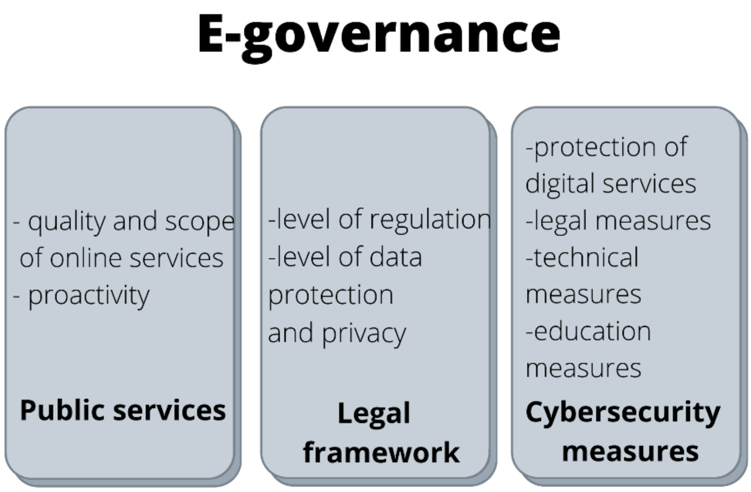
C) high-quality online public e-services that are proactive and ensure effective G2C and G2B communication.

2. Methodology

The theoretical model of the thesis stem from the legal approach- “law in books” (Pound, 1910). It refers to the fact that this paper will evaluate law as it is written in legal documents, not law as applied in practice. The approach “law in action” which refers to the practical application of law cannot be followed since it would require more advanced research tools that would exceed the needs of this thesis (Pound, 1910). The study scrutinizes three factors that are the primary determinants of the effectiveness of e-government in Slovakia through proposed indexes. For obtaining the most precise measurements of dependent and independent variables, a quantitative and qualitative research method will be used. To determine whether there is a causality between legal framework, cyber security, public e-services, and effectiveness of e-governance, a case study will be used since it will best serve the objectives of this research and reflects our incapacity to analyse the phenomenon on a larger scale.

E-governance could be defined as a manner of governmental execution of power through IT tools in order to ameliorate the state´s services offered to citizens and the private sector (Act no. 305/2013 Coll.). While myriad indicators influence e-governance, this thesis will focus on three major areas**: legal framework, cybersecurity measures, and public services.** The categories were formulated on the basis of studied literature, available data, and consultations with experts from public administration, the private sector, and academy.

Figure 1: Model of e-Government


E-governance

- quality and scope of online services
- proactivity
Public services

-level of regulation
-level of data protection and privacy
Legal framework

-protection of digital services
-legal measures
-technical measures
-education measures
Cybersecurity measures

The maximum points that the e-government could get is 100. Subsequently, it will be determined into which of the five categories evaluating the level of effective functioning the Slovak e-government falls. It was necessary to propose own categories since no other index measures effectiveness of e-governance. As indicated in Figure 2, the effectivity of e-government could be divided into the following categories: effective, functional, semi-functional, almost collapsing, and collapsing.

Figure 2: Effectivity of e-Government

E-gov	**Effective**	**Functional**	**Semi-functional**	**Almost collapsing**	**Collapsing**
Points	100-80	80-60	60-40	40-20	20-0

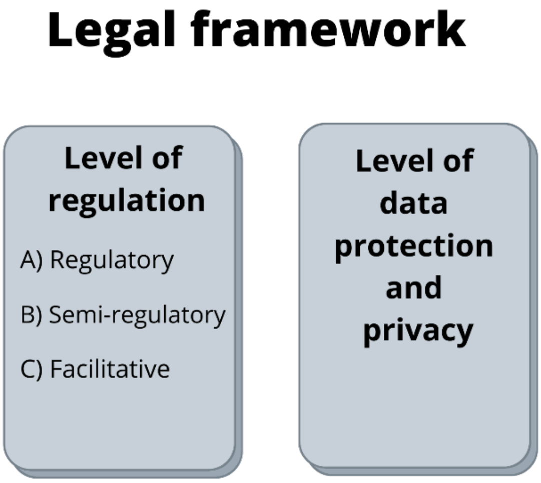
Every category will be evaluated and analysed separately through the indicators proposed in the Appendix. However, categories will not have equal weight. Greater emphasis must be given to the legal framework since it has the potential to either preclude or facilitate digitalization (Metcalf, 2019). For that reason, it will be attributed 50 points measured through proposed categories and indicators. Cybersecurity measures are inevitable for the successful adoption of digital policies by society. The perception of digital security is translated into a greater willingness to utilize e-services, and it positively impacts citizens' trust toward state institutions. Therefore, the maximum points for cybersecurity will account for 30 points. The last element- public e-services could have only 20 points since the bachelor thesis primarily focuses on synthesizing technical and legal solutions. Every indicator in a specific category will be assigned a different number of points based on its importance in the overall model.

Figure 3: Numerical Evaluation of Elements in e-Government

Elements of e-government	**Maximum points**
Legal framework	50
Cybersecurity measures	30
Public e-services	20

2.1 Legal Framework

Figure 4: Legal framework model



The legal framework lays down the fundamental principles of how the e-government will function, what its limitations will be, and whether security standards will be in place. It could both facilitate the implementation of e-policies or preclude progress in the digital realm. Therefore, the success or failure of digital policies is often determined by the formulation of legislature covering the informatization of society. The primary objective of a well-defined set of laws addressing digitalization should be to promote convergence between legal requirements, technological possibilities, and cyber security measures. In addition, the legal system is supposed to ensure that the misuse of political power will be limited. In case of infringements on data privacy, the perpetrators could be adequately punished.

Despite the demand for regulatory IT laws, opting for a more flexible legal system for e-governance is a desirable solution in the majority of cases. Three categories were established for measuring the adequacy of digital laws: **regulatory, facilitative, and semi-regulatory**. Proposed categories stem from Metcalf´s (2019) model, which suggests that law covering digital policies ought to have two functions: regulatory and facilitative. However, the reality is far more complex, and it would not be possible to divide the legal framework solely according to those two criteria. For that reason, a new category (semi-regulatory) must be created.

Regulatory laws prescribe exact procedures that must be respected when enacting specific policies in order to avoid data privacy violations and prevent security threats. The idea is similar to the European regulations that lay down the exact steps that ought to be taken by the member state. Regulatory laws do not leave space for broader interpretation or flexibility. On the other side of the spectrum lies a facilitative legal framework that ought to ensure broad possibilities for legal interpretation. This is necessary due to the rapid technological advancement since the specific law cannot keep pace with progress in the technological world due to an incomparably lower level of flexibility. Amending the law requires a more extended period which would preclude the state from adopting relevant digital policies that would reflect new technological developments. Facilitative laws are binding only on the objective, not on the manner of implementation. The intersection of these two would be semi-regulatory which does not have an over-regulatory function (it does not stipulate exact procedural steps that must be taken by the state), but the laws only stipulate specific processes that must be respected by state authorities when implementing e-policies.

Seven indicators **(e-signature, electronic delivery service, e-identification, authenticator, conversion, reference registers, electronic filing, and official electronic documents**) have been chosen to evaluate whether the specific elements of e-government law are formulated in a manner that would respect the proposed model, or whether they fall into different categories. Those indicators are an integral part of the Act on e-government. Maximum points for e-signature and e-ID are 5 which is slightly higher compared to other indicators. The reason is that without them the e-government could not function.

Figure 5: Indicator for measuring level of regulation

Indicator	Source	Max. points for indicator
E-signature	Act No. 305/2015	5
Electronic delivery service	Act No. 305/2015	4
E-identification	Act No. 305/2015	5
Authenticator	Act No. 305/2015	4
Electronic filing and electronic official documents	Act No. 305/2015	4
Conversion	Act No. 305/2015	4
Reference registers	Act No. 305/2015	4

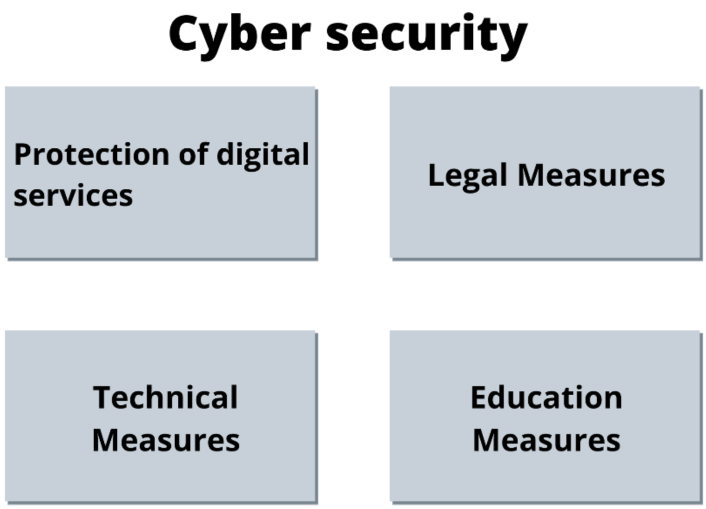
The second variable measured in the legal framework is the **level of data protection and privacy**. The level of data protection and privacy scrutinizes to what extent the measures aiming to protect the personal data of natural and legal persons and ensure the respect of the inherent right to privacy are taken. Data protection is indispensable to digital policies since citizens will not use e-services deemed insecure. Cyber incidents might violate the right to privacy, while unauthorized third parties may obtain sensitive information about citizens. Therefore, it is necessary to adopt a coherent set of laws and data protection legal measures that will preclude third parties from endangering the privacy and integrity of data. It is essential to establish a data protection authority that oversees all possible data privacy violations. The legal framework must also cover the situations when a cyber incident happens. The public administration should immediately inform affected entities about data breaches which should be a legal obligation. The penal code ought to cover data theft so that the perpetrators can be punished and affected parties compensated. Indicators in this category were taken from two prominent indexes: the National Cyber Security Index (NCSI) and Global Cybersecurity Index (GCI) (NSCI, n.d.; CGI, 2020). Personal data protection legislature and authority are absolute necessity for data protection and privacy framework. Therefore, the maximum points they could acquire is 5. Other categories

Figure 6: Indicators for measuring data protection and privacy

Indicator	Source	Max. points for indicator
Personal data protection legislature	NCSI	5
Personal data protection authority	NCSI	5
Laws on data theft	GSI	4
Personal data/privacy protection	GSI	4
Data breach notification	GSI	2

2.2 Cybersecurity Measures

Figure 7: Cybersecurity measures model



The legislature should address the issues emerging from potential threats and abuses of digital vulnerabilities. Security in e-services means that the assurance is given to citizens that their data and sensitive information are protected to a sufficient extent. The government must prevent both violations of data privacy and cyber-attacks conducted by third parties with the objective of accessing the sensitive data of citizens and classified information of the state. Therefore, cybersecurity measures refer to the ability of the state to deliver services that diverse cyber threats will not endanger.

Cybersecurity will be measured in four dimensions: **protection of digital services, legal measures, technical measures, and education measures**. These categories emanate from NCSI, GCI, and Digital Economy and Society Index (DESI) indexes that were complemented by indicators that published literature and experts assessed as crucial (*Global Cybersecurity Index 2020,* n.d.; NCSI, n.d.; *The Digital Economy and Society Index (DESI), n.d.*). Every question will be attributed one point from overall 30 points per cybersecurity measure. Education and legal measures constitute the largest part of cybersecurity measures. The research and data suggest that the most common cause of security incidents is the human factor. Therefore, it is necessary to educate public services users as well as all persons that are involved in the design, implementation, and enforcement processes.

Specific indicators in the protection of digital services category evaluate the extent to which the e-services offered by the state are safeguarded from external interference. Indicators in this section measure whether digital service providers have a legal obligation to incorporate generally recognized cybersecurity standards and implement cybersecurity requirements. Essential services should be protected, while the operators ought to have a legal obligation to manage cyber risks. State should establish the authority for overseeing cybersecurity and this authority should share information regarding potential cyber threats with its constituency.

Figure 8: Indicators for measuring protection of digital services

Indicator	Source	Max. points for indicator
CS digital service providers	NCSI	1
CS standard for public sector	NCSI	1
Supervisory authority	NCSI	1
Protection of essential services	NCSI	1
CS requirements for operators of essential services	NCSI	1
CSIRT- sectoral incident sharing	GCI	1

Indicators in legal measures examine the specific legal framework for cybersecurity of various parts of e-government. Legal measures ensure both the deterrence of possible abuses and the facilitation of law enforcement if an incident occurs. This part will evaluate whether there is a unique persistent identifier, timestamping, electronic delivery services, and supervisory authority in the state. The legal framework should incorporate internationally recognized cybersecurity standards while audits on the security of information systems are conducted on a regular basis. Laws ensure the identification of the following requirements for critical information infrastructure. The Penal Code covers illegal interception, interference, and access to devices, data, and computer systems.

Figure 9: Indicators for measuring legal measures

Indicator	Source	Max. points for indicator

Unique persistent identifier	NCSI	1
Timestamping	NCSI	1
Electronic delivery services	NCSI	1
Supervisory authority	NCSI	1
Implementation of standards	NCSI	1
Critical infrastructure	NCSI	1
Cybersecurity audit	GCI	1
Illegal interception on devices, computer systems and data	GCI	1
Illegal interferences on devices, data and computer system	GCI	1
Illegal access on devices, computer systems and data	GCI	1

Technical measures scrutinize the best technical practices that should ensure the cybersecurity of state information systems. The most important part of technical measures is the presence of a national CERT/CSIRT unit. This unit should provide information to the public regarding emerging cyber threats. Information sharing between authorities responsible for cybersecurity (CSIRT, CERT, MIRRI) in Slovakia cannot be neglected. Last but not least, the concept called security by design ought to be required by the law. It refers to a practise in which cybersecurity preventive measures are required right from the initial part of the project or solution implementation.

Figure 10: Indicators for measuring technical measures

Indicator	Source	Points for indicator
CSIRT/CERT	NCSI	1
CSIRT/CERT advisories	GCI	1
Security by design	Expert consultation	1
MIRRI, CERT, CSIRT information sharing	Expert consultation	1

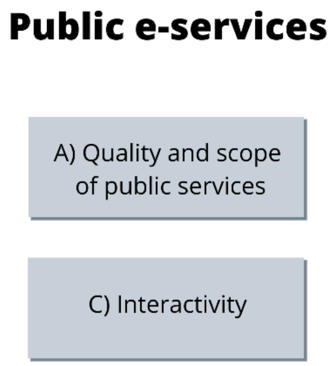
Education measures evaluate whether state authorities conduct awareness campaigns and educational programs designated for primary, secondary, and high school students as well as for the elderly, persons with special needs, civil society, the broader public, public administration, and experts on law enforcement and other judicial and legal actors.

Figure 11: Indicators for measuring education measures

Indicator	**Source**	**Points for indicator**
CS awareness activities	Expert consultation	1
CS primary and secondary education	NCSI	1
CS high school education	NCSI	1
CS older generation	GSI	1
CS civil society	GSI	1
CS citizens	GCI	1
CS persons with special needs	GCI	1
CS judicial and legal actors	GCI	1
CS law enforcement	GCI	1
CS public sector/governmental officials	GCI	1

2.3 Public e-Services

Figure 12: Public e-services model



High-quality public services are an indispensable part of well-functioning e-government. E-services could be defined as any service offered by public authorities in digital form. Online public services must be accessible to citizens and must alleviate problems emanating from the government to citizen (G2C) and government-to-business (G2B) communication. The major purpose of the electronic exercise of public administration is to provide citizens with services that would facilitate communication with the state, which should result in enhanced well-being of individuals. As suggested in figure 6, this variable will be measured through the **quality and scope of online services** and **the proactivity** of digital communication. Categories were formulated based on the research, DESI index, eGovernment Benchmark, and consultations with public administration authorities (*The Digital Economy and Society Index,* n.d; European Commission, 2021).

The quality and scope of public services evaluate the extent to which the e-services are available and accessible to digital service users. Two indicators measure whether at least 70% of services for citizens and the private sector are provided online. If the state already possesses user data, it should be reflected in offering a pre-filled form to users in at least 60% of cases. An indispensable part of e-services is the level of interaction. This indicator will evaluate whether the number of individuals using online communication with the state exceeds 70%. The last two indicators from Figure 13 measure the percentage of services with a mobile-friendly interface and online support. All indicators emanate from DESI and e-

Government Benchmark indexes (*The Digital Economy and Society Index,* n.d; European Commission, 2021).

Figure 13: Indicators for measuring quality and scope of e-services

Indicator	Source	Points for indicator
Public e-services for citizens	DESI	2
Public e-services for businesses	DESI	2
Pre-filled forms	DESI	2
Interaction with the state	DESI	2
Mobile friendliness	eGov Benchmark	3
User support	eGov Benchmark	3

Proactivity refers to the state practice which ensures that the state does not require the citizen to make an input to deliver a service. Suppose the state already possesses all the needed information for taking the initiative. In that case, the state delivers a service that fulfils the legal obligation of the user instead of requiring a citizen to take the first action. However, the first step should ensure that the "once only" approach is respected. It refers to the fact that the state should not ask a citizen to provide the same information twice, but once the information about the citizen enters state information systems, the state should internally exchange that information.

Figure 14: Indicators for measuring proactivity of e-services

Indicator	Source	Points for indicator
Input from citizens	Expert consultations	2
Proactive services	Expert consultations	2
Once only approach	Expert consultations	2

3. Digital Slovakia

In this chapter, the functioning of e-government in Slovakia is evaluated through three major components —legal framework, cybersecurity measures, and public e-services. Every component contains several indicators that can be found in the appendix. Each indicator is followingly evaluated separately through the national legislature and institutional competencies. Data originate from existing indexes (NCSI, DESI, GCI, eGovernment Benchmark), national legislation, and consultations with experts supported by evidence referring to laws and specific activities conducted by state institutions. Subchapters contain comprehensive tables indicating the final number of points for each element as well as the overall assessment of three components. The analysis indicates which elements function well and which hinder the effective functioning of e-government and hence should be ameliorated. This chapter assesses only the components on its own, while the overall evaluation of Slovak e-government will follow in the next chapter.

3.1 Legal Framework for Slovak e-Government

Legal framework performs 38 out of 50.

Figure 15: Table Evaluating Components of Legal Framework

Element	**Points**
Data protection and privacy	20/20
Level of regulation	18/30

The data evaluation indicates that the legal framework covering e-government is relatively effective. The law protects the data of all entities involved in electronic communication with the state to a sufficient extent. Legal framework from the data protection and privacy perspective scores 20 out of 20. Therefore, it could be concluded that the data of individuals are legally protected to a sufficient extent. Slovakia has enacted legislation on data protection and privacy which stems from the European General Data Protection Regulation (Regulation 2016/679). In the case of a data breach, the state is required to notify affected parties about the incident and the laws on data theft are in force (Act No. 69/2018 Coll.; Act No. 305/2005 Coll.). Moreover, Slovakia established a Personal Data Protection authority that oversees the protection of sensitive personal information about natural persons (*O nás, n.d*).

Slightly more problematic is the part on the level of regulation. This part attained 18 out of 30 points due to the overregulation of the three indicators – authenticator, reference registers, and electronic delivery services. Even though it is not absolutely necessary to stipulate exact procedural steps that ought to be taken when anyone works with these indicators, the authorities decided to regulate them. Regulation is desirable in certain parts of e-government law due to the security reasons and accountability of the actors. However, when it comes to authenticator, reference registers, and electronic delivery services, it would be possible to stipulate solely the objective and certain procedural steps without infringing security. Therefore, those three indicators should be in the category of semi-regulatory instead of regulatory. As Metcalf (2019) suggested, e-ID and e-signature should be regulated to a greater extent so that the users would be granted security when interacting with the state in a digital realm. In the case of Slovakia, both e-ID and e-signature fall into the category of the regulatory legal framework. Electronic filing and official documents must be regulatory due to the fact that the users could be under certain conditions punished for not properly using those services. The users must know what behaviour is expected from them when interacting with a state online. For that reason, the overregulation in the case of those two indicators could be justified. The same is valid for conversion since the legal text ought to stipulate exact procedural steps, so the conversion would be considered legally valid.

3.2 Security of e-Government in Slovakia

Cybersecurity measures perform 22 out of 30.

Figure 16: Table Evaluating Components of Cybersecurity Measures

Element	**Points**
Protection of digital services	6/6
Legal measures	9/10
Technical measures	4/4
Education measures	5/10

Digital services could be deemed secure since the legislation provides for sufficient protection measures. This element acquired 6 points out of 6. The law requires digital service providers to adopt cybersecurity measures (Act No. 69/2018 Coll.). Essential service operators are identified and are required to manage cyber and ICT risks (Act No. 69/2018 Coll.). Sectoral CSIRT operating under MIRRI has an obligation to share information with the public regarding cyber threats and the desirable preventive actions (Act No. 69/2018 Coll.). The national CERT was established under National Security Authority in 2016 and oversees all cyber incidents within the state. Furthermore, technical cybersecurity measures are of high quality since all indicators acquired total points. The legal framework requires the implementation of best technical security practices, such as the approach called “security by design” (Act No. 95/2019 Coll.) It refers to a practice that requires the implementation of security measures right from the very beginning of the e-solution implementation. Slovakia has national CERT and sectoral CSIRT, which shares information regarding emerging cyber with its constituency (Act No. 69/2018 Coll.).

Moreover, the effective internal communication among state actors involved in implementing and protecting digital services, which is inevitable for functional state services, is present in legislative obligations (Act No. 69/2018 Coll.). Legal measures attained 9 out of 10 points which could be deemed sufficient legal coverage of cybersecurity. Slovak legal framework, *inter alia,* regulates unique identifiers, timestamping, and electronic registered delivery services. Slovakia has enacted legislation on illegal access, interference, and interception of devices, computer systems, and data (Act No. 305/2005 Coll.). The state has competent supervisory authority for qualified trust service providers, and critical information infrastructure is identified (Act No 45/2011 Coll.; Act No. 69/2018 Coll.). The state is required to periodically evaluate the information system´s security (Act No. 69/2018 Coll.). The only indicator in Slovakia that cannot be found is the integration of international cybersecurity standards into domestic legislation. It must be noted that this is a non-standard approach since the integration of international standards could considerably increase level of cybersecurity.

On the contrary, Slovakia is failing in cybersecurity education measures. The human factor is the most common cause of cyber incidents. It is, therefore, desirable for the state to educate users and individuals involved in policy-making processes on cybersecurity competencies. Only when nationwide awareness campaigns targeting citizens, the private sector, and public administration officials are conducted can digital solutions be deemed secure. Despite effective legal and technical cybersecurity measures, digital state infrastructure will not be secure without cybersecurity awareness among users.

Education must begin with the youngest generation. They are the future users of e-services, and hence it is necessary to include fundamental cybersecurity competencies in school curricula. Neither high school students nor elementary and primary school students acquire knowledge of secure behaviour in the digital realm. The most vulnerable groups in online space (people with special needs and the elderly) should be given special attention in cybersecurity education. However, Slovakia does not provide any awareness or educational activities targeting those groups. Slovakia also lacks educational cybersecurity campaigns that would be sector-specific. Civil society has no possibility to attend courses or training in cybersecurity competencies from the state, although they are an integral part of the state's information infrastructure. Three exceptions could be observed in training for the public sector, legal actors, and law enforcement authorities provided by the state (*Študijný Plán Rok 2022*, n.d.). Cyber awareness campaigns on a national scale are conducted but with very limited outreach (Cybergame, n.d).

3.3 Slovak e-Services

Public e-services perform at 9 out of 20 points.

Figure 17: Table Evaluating Components of Public e-Services

Element	Points
Quality and scope of public e-services	8/14
Proactivity	1/6

The performance of Slovak public e-services indicates that there is a considerably large space for improvement. Digital services are of average quality, scoring 8 out of 14. While the services are generally mobile-friendly and user supportive, they are provided to a greater extent only for the business sector (*The Digital Economy and Society index,* n.d.). Citizens are often deprived of online public services and cannot interact with public authorities in the digital realm (*The Digital Economy and Society index,* n.d.). Sharing information about users of e-services and their data is insufficient, which is reflected in the failure to offer pre-filled forms to e-service users (European Commission, 2021).

In addition, the Slovak state still acts as a reactive entity—the state requires input from the citizen and only afterward provides service. There are various cases when the state is aware of the fact that the user will need a public service; the state already possesses all the information necessary to act but fails to do so. There are attempts by the Slovak Ministry of Investments, Regional Development and Informatization (MIRRI) to change this paradigm. A most notable one is the introduction of so-called “life events”—the common situation that a citizen might encounter. Even though MIRRI has announced 16 life events, a specific vision for their implementation has been introduced only for two of them—losing and searching for employment and purchase of non-movable property for a living (*Zaujíma Nás Váš Názor,* 2022). The situation could be ameliorated by the application called Slovakia in a Mobile (Slovensko v mobile), which became available to the public a few months ago but still awaits the installation of all announced functionalities. Furthermore, the law does not require implementing the once-only approach. It refers to the fact that public administration does not share information about individuals that enter the state information systems. Databases are not interoperable, constituting the most prominent obstacle in information-sharing processes. If the databases of state institutions are not interoperable and hence allow the execution of once only one approach, the state cannot become a proactive entity. In conclusion, public e-services are the major obstacle that precludes the effective functioning of e-government in Slovakia.

4. Evaluation of e-Governance in Slovakia

E-government perform 71 out of 100 points.

Figure 18: Table evaluating components of e-government

Component	Element	Points
1. Legal framework		
	Data protection and privacy	20/20
	Legal measures	18/30
		38/50
2. Cybersecurity measures		
	Protection of digital services	6/6
	Legal measures	9/10
	Technical measures	4/4
	Education measures	5/10
		24/30
3. **Public e-services**		
	Quality and scope of public e-services	8/14
	Proactivity	1/6
		9/20

The overall performance of e-government in Slovakia falls into the category **of functional**, which was established in the methodology. The legal framework functions effectively and covers a broad range of elements that are *sine qua non* for e-government. The initial assumption that the components of e-government law are overly more regulatory than they ought to be, which tends to preclude the effective functioning of e-government, was partly proven wrong. Even though authenticator, electronic delivery service, and reference registers were regulated to a greater extent than was necessary, the other four chosen elements were adequately regulated. However, it does not lead to a conclusion that the digital laws related to e-government are adequately regulated in general. For the purposes of this study, only seven elements were analysed, which does not serve as a representative sample for generalization.

From the cybersecurity perspective, it could be concluded that digital services are secure while technical and legal measures are of the highest standards. The only problematic part of cybersecurity measures is education. The state does not provide sufficient education opportunities for any age and professional group. Some attempts to improve the situation could be observed, mainly stated in the Slovak Cybersecurity Strategy 2021-2025 and following Action Plan but so far without any tangible results (National Security Authority, 2021). E-government cannot be deemed secure if the actors involved in digital communication with the state are not adequately educated in safe online behaviour. The human factor is considered the highest threat to cybersecurity. It must be noted that all cybersecurity measures were evaluated based on existing legal frameworks. However, the practices, in reality, might dramatically differ.

The major obstacle that precludes the effective functioning of e-government in Slovakia is public e-services. The quality and scope of the digital services provided for the entities interacting with the state authorities are fairly low. The users cannot expect high-quality online services while they are required to enter the same information that the state already possesses over and over again. Slovak state still acts as a reactive entity and waits until action is requested from the user instead of proactively offering services that the users will, by necessity, need. There are some attempts to shift this paradigm through “life events,” but it could be considered only a small step in this direction.

It could be concluded that the Slovak e-government is functional, while certain aspects could be ameliorated in the future. Most notably, public e-services and educational measures in cybersecurity should be given greater emphasis. The legal framework covering e-government, data protection, and cybersecurity is well-formulated and covers a broad range of areas, but it could be less regulatory in certain instances.

5. Concluding Remarks

This thesis revealed that the most significant obstacles that hamper progress in the effective functioning of e-government are low quality public e-services, insufficient cybersecurity education measures, and high regulation level of legislation. Therefore, policymakers, in the first place, ought to give greater emphasis to the amelioration of public e-services. Even though attempts to offer more proactive services could be observed, it is only a first step that should be followed by others with the same objective. The initial step must be to require "once only" approach to be implemented so that the users do not have to enter the same information several times. To make this step possible, databases should be interoperable to facilitate the exchange of information. Furthermore, the scope of digital services could be improved, while the aim should be to increase the number of digital services users.

Education measures are an indispensable part of digitalization. When citizens do not have digital skills and are not aware of the potential threats in the digital realm, the implementation of e-policies will never be successful. The policies should primarily focus on the cyber education of the youngest generation since they are the future users of those services. Digital and cyber skills should be a cornerstone of primary, secondary, and high school education. Moreover, the vulnerable groups ought to be given special attention in cyber competencies since they are the easiest targets of attackers. The elderly and persons with special needs face many obstacles in the digital realm. For that reason, it is necessary to offer training in cyber competencies and digital skills that would allow them to use e-services. Lawyers, judges, and other legal actors should be educated in fundamental cyber competencies since more and more cases will include cyber-related issues.

In addition, state legal experts should consider the level of regulation whenever amending the digital law or proposing a new one since overregulation tends to hinder progress in digitalization. This innovative approach of differentiating between regulatory and facilitative laws should become a new standard for public administration when dealing with e-government and other aspects of digitalization. The legal framework as it is written in laws seems to be sufficient, but further study on how it is reflected and implemented in reality ought to be conducted. The results of this study and the metrics from other technological indexes do not seem to correspond with the experiences of individuals and companies. Therefore, it would be desirable to enlarge this thesis by the "law in action" approach that would measure the actual situation regarding the functioning of e-government not as they are written in laws but as they are practiced in daily reality. Slovakia is well known for its myriad strategies and action plans, but the government is not always capable of fulfilling its objectives. Having a legal obligation is not necessarily always translated into the enforcement of this obligation. Therefore, the research comparing the measured functioning of e-government and practical realization would be desirable.

The story of digitalization is not only about having more effective public administration and improving the communication with the state. It is first of all about ensuring that the democratic principles and human rights will be respected in digital age. For thirty years, Slovakia has been struggling with democratization which is reflected in low trust towards institutions, omnipresent corruption, lack of transparency, and other negative phenomena. Digitalization of public administration is therefore a plausible solution for ensuring that the quality of democracy in Slovakia will be improved. E-government has a potential to eradicate inequalities, create more inclusive environments for all citizens, lower the bureaucratic complexity, and reduce corruption. The most important benefit of e-government is that it could increase the trust towards institutions. After the years of disappointments in political elites and unfunctional democracy, digitalization of public administration offers many possibilities for improving democracy in Slovakia. The only question that remains to be answered is what story Slovakia decides to write.

Resumé

Digitalizácia verejnej správy je na Slovensku témou, o ktorej je vo verejnom diskurze počuť len málo. Je pritom absolútne nevyhnutná pre redukciu korupcie, zvýšenie miery transparentnosti pri spravovaní vecí verejných, zníženie byrokratickej náročnosti a s tým súvisiace celkové zlepšenie kvality demokracie, s ktorou Slovensko už roky zápasí. Táto bakalárska práca preto skúma elementy nevyhnutné pre efektívne fungovanie e-governmnetu na Slovensku. Hoci na elektronický výkon verejnej moci vplýva množstvo faktorov, je potrebné klásť dôraz na tri hlavné aspekty určujúce úspech e-governmentu. Právny rámec musí byť garanciou bezpečnosti a súkromia dát používateľov a musí taktiež prepájať technologické možnosti s tými právnymi. E-politiky musia byť navrhované spôsobom, aby spĺňali najvyššie kyberbezpečnostné štandardy. V neposlednom rade by mal štát poskytovať elektronické služby, ktoré budú kvalitné a proaktívne.

Empirická časť hodnotí efektivitu fungovania e-governmentu na Slovensku. Efektivita sa meria prostredníctvom vytvoreného modelu pozostávajúceho z troch hlavných elementov: právny rámec, kyberbezpečnostné opatrenia a verejné e-služby. Model je zároveň postavení na právnej doktríne „právo v knihách“, teda prístupe hovoriacom o skúmaní právnych praktík ako sú napísané v zákonoch, nie o tom ako sa prakticky aplikujú. Vyhodnotenie efektivity fungovania e-governmentu následne prebieha cez uvedené elementy merané prostredníctvom indikátorov prevzatých z už existujúcich indexov rovnako ako aj indikátorov navrhnutých odborníkmi v danej oblasti. Časť práce o právnom rámci sa pozerá na mieru regulácie zákonov a mieru ochrany a súkromia dát. Kyberbezpečnostné opatrenia sa zameriavajú na technické, právne a vzdelávacie opatrenia ako aj ochranu digitálnych služieb. Pri e-službách sa vyhodnocuje kvalita, rozsah a proaktivita verejných služieb.

Právny rámec získal 38 bodov z celkových 50. Hlavnou prekážkou v tejto časti bola prehnaná regulácia zákonov týkajúcich sa elektronického výkonu verejnej moci. Zákonodarcovia totiž mnohokrát nie sú oboznámený s inovatívnym prístupom k regulácii technológií, ktorý v istých prípadoch preferuje väčšiu mieru flexibility v rámci interpretácie zákona. Je tiež potrebné poznamenať, že ochrana a súkromie dát sú zákonmi kvalitne pokryté. Kyberbezpečnostné opatrenia sú vo všeobecnosti efektívne, pričom získali hodnotenie 22 bodov z 30. Technické a právne opatrenia dosahujú najvyššie štandardy a spolu s ochranou digitálnych služieb tvoria kvalitný základ pre kyberneticky bezpečnú štátnu infraštruktúru. Problémom však zostáva nedostatočné vzdelávanie rôznych skupín občanov ako aj expertov. Ľudský faktor je pritom najčastejšou príčinou kyberbezpečnostných incidentov. Kyberbezpečnostné opatrenia preto nemôžu byť považované za dostačujúce aj napriek pomerne vysokému hodnoteniu. Poslednou, a zároveň najslabšou stránkou e-governmentu, sú verejné e-služby. Tie získali 9 bodov z 20, keďže majú nedostatočnú kvalitu a rozsah, pričom príklady dobrej praxe ukazujú, že e-služby by mali byť v prvom rade proaktívne. Slovenské e-služby však zaostávajú vo všetkých ohľadoch.

Práca na záver hodnotí, že slovenský e-government je funkčný, keďže získal 71 bodov zo 100. Tvorcovia politík by sa mali zamerať na úroveň regulácie zákonov, verejné e-služby, a vzdelávacie opatrenia v oblasti kybernetickej bezpečnosti. Práca taktiež vyzýva k ďalšiemu komparatívnemu výskumu, ktorý by porovnal rozdiel medzi nastavením právneho rámca e-governmentu a praktickou implementáciou zákonných povinností a jeho fungovaním v praxi. Je totiž vysoko pravdepodobné, že výsledky merania e-governmentu v praxi sa budú značne líšiť od jeho fungovania na papieri. Cieľom práce bolo zmerať fungovanie e-governmentu na Slovensku prostredníctvom nastavenej legislatívy, čo môže slúžiť ako odrazový mostík do ďalšieho výskumu.

List of references

Act No 45/2011 Coll., Act on Critical Infrastructure. (2011). https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2011/45/20210301

Act No. 305/2013 Coll.**,** Act on Electronic Form of Exercise of the Powers of Public Authorities and on Amendments and Supplements to certain Acts (Act on e-Government). (2013). https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2013/305/20180401

Act No. 69/2018 Coll., Act on Cybersecurity and on Amendments and Supplements to certain Acts (2018). https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/69/

Act No. 305/2005 Coll., Penal Code (2005). https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2005/300/20220717

Act No. 95/2019 Coll., Act on Information Technologies of Public Administration and Supplements to certain Acts (2019). https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2019/95/20190501.html

Adams, M. & Prins, C. (2017). Digitalization through the lens of law and democracy. In C. Prins, C. Cuijpers, P. L. Lindseth, & M. Rosina (Eds.), *Digital democracy in a globalized world* (pp. 3-23). (Elgar Law, Technology and Society). Edward Elgar.

Andersson, A. & Twizeymana, J. D. (2019). The public value of E-Government – A literature review. Government Information Quarterly 36(2), pp. 167-178.

CYBERGAME. (n.d.). Retrieved January 20, 2023, from https://cybergame.sk-cert.sk/

Dutt, P.K & Kerikmäe, T. (2014). Concepts and Problems Associated with eDemocracy. In: Kerikmäe, T (eds) Regulationg eTechnologies in the European Union. Springer International Publishing Switzerland. https://doi.org/10.1007/978-3-319-08117-5_13

European Commission. (2021). eGovernment Benchmark 2021: Entering a New Digital Government Era.

Global Cybersecurity Index 2020. (n.d.). Retrieved November 29, 2022, from https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E

Hartanto, D., Dalle, J., Akrim, A. & Anisah, H.U. (2021). Perceived effectiveness of e-governance as an underlying mechanism between good governance and public trust: a case of Indonesia. *Digital Policy, Regulation and Governance*, *23(6),* pp. 598-616.

Metcalf, K. N. (2019). How to build e-governance in a digital society: The case of Estonia*. Revista Catalana de Dret Públic, 58*.

Metcalf, K. N. (2014). E-governance in law and by law: The legal framework of e-governance. Retrieved June 13, from https://www.researchgate.net/publication/298718938_E-governance_in_law_and_by_law_The_legal_framework_of_e-governance

National Security Authority. (2021). *The National Cybersecurity Strategy 2021-2025.* https://www.nbu.gov.sk/wp-content/uploads/cyber-security/National_cybersecurity_strategy_2021.pdf

NCSI. (n.d.). Retrieved November 29, 2022, from https://ncsi.ega.ee/ncsi-index/

O Nás. Úrad na ochranu osobných údajov Slovenskej republiky. (n.d.). Retrieved December 13, 2022, from https://dataprotection.gov.sk/uoou/sk/main-content/o-nas

Pound, R. (1910). Law in Books and Law in Action. *American law Review 44.*

Regulation 2016/679. the protection of natural persons with regard to the processing of personal data and on the free movement of such data. Retrieved December 13, from https://eur-lex.europa.eu/eli/reg/2016/679/oj

Shim, D.C. & Eom, T.H. (2008). E-Government and Anti-Corruption: Empirical Analysis of International Data. *International Journal of Public Administration* 31(3), pp. 298-316.

Strážovská, Ľ. & Ďuriš, M. (2018). Digitalization of society and e-Government. Retrieved June 13, from https://www.researchgate.net/publication/344858050_Digitalization_of_Society_and_e-Government

Študijný Plán Rok 2022. (n.d.). Retrieved January 20, 2023, from https://ja-sr.sk/sites/default/files/Studijny_plan_2022_schvaleny.pdf

The Digital Economy and Society index (DESI). Shaping Europe's digital future. (n.d.). Retrieved November 29, 2022, from https://digital-strategy.ec.europa.eu/en/policies/desi

Zaujíma Nás Váš Názor: Predstavujeme podobu dvoch životných Situácií. Ministerstvo investícií, regionálneho rozvoja a informatizácie SR. (2022, November 30). Retrieved January 3, 2023, from https://www.mirri.gov.sk/aktuality/plan-obnovy-a-odolnosti/predstavujeme-viziu-dalsich-dvoch-zivotnych-situacii-privitame-vas-nazor/index.html

Appendices

Legal framework

Data protection and privacy		
Personal data protection legislature (5/5) **Criteria** There is a legal act for personal data protection.	**Yes** No	**Evidence** Legal act https://dataprotection.gov.sk/uoou/en/content/national-legal-framework https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2013/122/20140415
Personal data protection authority (5/5) **Criteria** There is an independent public supervisory authority that is responsible for personal data protection.	**Yes** No	**Evidence** Official website and legal act https://dataprotection.gov.sk/uoou/en https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2013/122/20140415
Substantive laws on data theft (4/4) **Criteria** Online identity theft- stealing personal information such as names, addresses, date of birth, contact information or bank account. Can occur as a result of phishing, hacking online accounts, retrieving information from social media or illegal access to databases.	**Yes** No	**Evidence** Legal act https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2005/300/20220717
Personal data/ privacy protection (4/4) **Criteria**	**Yes** No	**Evidence** Legal act https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/18/

Regulations about protection personal data from unauthorized access, alteration, destruction, or use. Internet privacy and security level of personal data published via Internet. It is a broad term that refers to variety of factors, techniques and technologies used to protect sensitive and private data, communication, and preferences.		
Data breach notification (2/2) **Criteria** Breach notification laws or regulations are ones that require an entity that has been subject to a breach to notify authorities, their customer and other parties about the breach, and take other steps to remediate injuries caused by the breach. These laws are enacted in response to an escalating number of breaches of consumer databases containing personally identifiable information.	**Yes** No	**Evidence** Legal act https://www.sk-cert.sk/wp-content/uploads/2018/03/2018_69-Act-on-Cybersecurity.pdf
Level of regulation		
E-signature (5/5)	**What is the regulation level of abovementioned element?** Facilitative Semi-regulatory **Regulatory**	**According to theoretical framework, in which category the element should be?** Facilitative Semi-regulatory **Regulatory**
Electronic delivery service (0/4)	**What is the regulation level of abovementioned element?** Facilitative Semi-regulatory	**According to theoretical framework, in which category the element should be?** Facilitative

	Regulatory	**Semi-regulatory** Regulatory
E-identification (5/5)	**What is the regulation level of abovementioned element?** Facilitative Semi-regulatory **Regulatory**	**According to theoretical framework, in which category the element should be?** Facilitative Semi-regulatory **Regulatory**
Authenticator (0/4)	**What is the regulation level of abovementioned element?** Facilitative Semi-regulatory **Regulatory**	**According to theoretical framework, in which category the element should be?** Facilitative **Semi-regulatory** Regulatory
Electronic filing and electronic official document (4/4)	**What is the regulation level of abovementioned element?** Facilitative **Semi-regulatory** Regulatory	**According to theoretical framework, in which category the element should be?** Facilitative **Semi-regulatory** Regulatory
Conversion (4/4)	**What is the regulation level of abovementioned element?** Facilitative Semi-regulatory **Regulatory**	**According to theoretical framework, in which category the element should be?** Facilitative Semi-regulatory **Regulatory**
Reference registers (0/4)	**What is the regulation level of abovementioned element?** Facilitative Semi-regulatory	**According to theoretical framework, in which category the element should be?** Facilitative **Semi-regulatory**

	Regulatory	Regulatory

Cybersecurity measures

Protection of digital services		
1.1 **Cyber security responsibility for digital service providers (1/1)** **Criteria** According to the legislation, digital service providers (except micro and small enterprises): (1) must manage cyber/ICT risks or (2) must implement established cyber/information security requirements	**Yes** No	**Evidence** Legal act https://www.sk-cert.sk/wp-content/uploads/2018/03/2018_69-Act-on-Cybersecurity.pdf
1.2 **Cyber security standard for the public sector (1/1)** **Criteria** Public sector digital service providers must implement (1) cyber/ICT security requirements (defined by legislation) or (2) a widely recognised security standard.	**Yes** No	**Evidence** Legal act https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2014/55/20200501
Competent supervisory authority (1/1) **Criteria** The government has a competent authority in the field of cyber/information security that has the power to supervise public and private digital service providers regarding the implementation of cyber/ information security requirements	**Yes** No	**Evidence** Legal act https://www.sk-cert.sk/wp-content/uploads/2018/03/2018_69-Act-on-Cybersecurity.pdf
Protection of essential services (1/1) **Criteria**	**Yes** No	**Evidence** Legal act

There is a legal act that allows to identify operators of essential services.		https://www.sk-cert.sk/wp-content/uploads/2018/03/2018_69-Act-on-Cybersecurity.pdf
Cyber security requirements for operators of essential services (1/1) **Criteria** According to the legislation, operators of essential services must manage cyber/ICT risks.	**Yes** No	**Evidence** Legal act https://www.sk-cert.sk/wp-content/uploads/2018/03/2018_69-Act-on-Cybersecurity.pdf
CSIRT shares sectoral incidents within its constituency (1/1) **Criteria** Sharing of information on emerging cyberthreats and the recommended actions to take.	**Yes** No	**Evidence** Legal act https://www.sk-cert.sk/wp-content/uploads/2018/03/2018_69-Act-on-Cybersecurity.pdf
Legal measures		
Unique persistent identifier (1/1) **Criteria** The government provides a unique persistent identifier to all citizens, residents, and legal entities. For example, identifier remains the same after documents expiration and name change.	**Yes** No	**Evidence** Legal act https://www-epi-sk.translate.goog/zz/1995-301?_x_tr_sl=sk&_x_tr_tl=en&_x_tr_hl=en
Timestamping (1/1) **Criteria** Timestamping is regulated	**Yes** No	**Evidence** Legal act https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014R0910&
Electronic registered delivery services (1/1) **Criteria**	**Yes** No	**Evidence** Legal act

Electronic registered delivery service between state entities, citizens and private sector entities is regulated. The service provides legally binding data exchange and guarantees the confidentiality and integrity of information		https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014R0910&f
Competent supervisory authority (1/1) **Criteria** There is an authority responsible for the supervision of qualified trust service providers.	**Yes** No	**Evidence** Official website https://www.nbu.gov.sk/en/trust-services/supervision-schemes/index.html
Implementation of standards (0/1) **Criteria** Existence of a government-approved (or endorsed) framework (or frameworks) for the implementation of internationally recognized cybersecurity standards within the public sector (government agencies) and within critical infrastructure (even if operated by private sector). These standards include, but are not limited to those developed by the following agencies: ISO, ITU, IETF, IEEE, ATIS, OASIS, 3GPP, 3GPP2, IAB, ISOC, ISG, ISI, ETSI, ISF, RFC, ISA, IEC, NERC, NIST, FIPS, PCI DSS, etc.	Yes **No**	**Evidence**
Identification and protection of national critical information infrastructure (1/1) **Criteria** Critical infrastructure constitutes basic systems crucial for safety, security, economic security, and public health of a nation. Those systems may include, but are not limited to defence systems, banking and	**Yes** No	**Evidence** https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2011/45/20210301

finance, telecommunication, energy and other.		
Cybersecurity audit requirements (1/1) **Criteria** A security audit means a systematic and periodic evaluation of information system´s security.	**Yes** No	**Evidence** Legal act https://www.sk-cert.sk/wp-content/uploads/2018/03/2018_69-Act-on-Cybersecurity.pdf
Substantive laws on illegal interception on devices, computer systems and data (1/1) **Criteria** Illegal interception- both intentional and unauthorized, non-public transmission of computer data to, from or within a computer or another electronic system, made by technical means.	**Yes** No	**Evidence** Legal act https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2005/300/20220717
Substantive law on illegal interferences (through data input, alteration, and suppression) on devices, data and computer system? (1/1) **Criteria** Computer system interference- both intentional and unauthorized serious hindering of the functioning of a computer system. It might include inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data. Data interference either intentional and unauthorized damaging, deletion, deterioration, alteration, or suppression of computer data.	**Yes** No	**Evidence** Legal act https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2005/300/20220717

Substantive law on illegal access on devices, computer systems and data (1/1) **Criteria** Access- the ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components, and functions (NICCS). Computer system or system- any device or a group of interconnected or related devices, one or more which, pursuant to a program, perform automatic processing of data (COE- Convention on Cybercrime). Computer data- any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function (COE)	**Yes** No	**Evidence** Legal act https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2005/300/20220717
Technical measures		
National/government CIRT/CSIRT/CERT (1/1) **Criteria** Supported by a government´s decision or is part of governmental or national structures.	**Yes** No	**Evidence** Official website https://www.csirt.gov.sk/ https://www.cert.gov.sk/sk/uvod/
National/government CIRT/CSIRT/CERT – publicly available advisories (1/1) **Criteria** Sharing of information with general public on emerging cyberthreats and the recommended actions to take.	**Yes** No	**Evidence** Legal act https://www.sk-cert.sk/wp-content/uploads/2018/03/2018_69-Act-on-Cybersecurity.pdf

Security by design (1/1) **Criteria** It is required for public authorities to adopt cybersecurity measures when implementing digital solutions.	**Yes** No	**Evidence** Legal act https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2019/95/20190501.html
MIRRI, CSIRT and CERT information sharing (G2G communication) (1/1) **Criteria** Authorities responsible for public e-services are required to internally share information about emerging cyberthreats and cyber incidents.	**Yes** No	**Evidence** Legal act https://www.sk-cert.sk/wp-content/uploads/2018/03/2018_69-Act-on-Cybersecurity.pdf
Education measures		
National/government CIRT/CSIRT/CERT-cybersecurity awareness activities (1/1) **Criteria** State institutions organize nation-wide cybersecurity awareness campaigns in order to enhance cyber safety competencies.	**Yes** No	**Evidence** www.sk-cert.sk https://cybergame.sk-cert.sk/
Cyber safety competencies in primary or secondary education (0/1) **Criteria** Primary or secondary education curricula include cyber safety/ computer safety competences.	Yes **No**	**Evidence**
Cyber safety competencies in high school education (0/1) **Criteria**	Yes **No**	**Evidence**

High school education curricula include cyber safety/ computer safety competences.		
Cyber safety competencies of older generation (0/1)	Yes **No**	**Evidence**
Public awareness campaigns targeting civil society (0/1)	Yes **No**	**Evidence**
Public awareness campaigns targeting citizens (1/1)	**Yes** No	**Evidence** https://cybergame.sk-cert.sk/
Public awareness campaigns targeting persons with special needs (0/1)	Yes **No**	**Evidence**
National sector-specific educational programmes/trainings/courses for judicial and other legal actors (1/1)	**Yes** No	**Evidence** https://www.nbu.gov.sk/wp-content/uploads/kyberneticka-bezpecnost/Akcny-plan-kybernetickej-bezpecnosti.pdf
National sector-specific educational programmes/trainings/courses for law enforcement (1/1)	**Yes** No	**Evidence** https://www.nbu.gov.sk/wp-content/uploads/kyberneticka-bezpecnost/Akcny-plan-kybernetickej-bezpecnosti.pdf
National sector-specific educational programmes/trainings/courses for other public sector/governmental officials (1/1)	**Yes** No	**Evidence** https://www.nbu.gov.sk/wp-content/uploads/kyberneticka-bezpecnost/Akcny-plan-kybernetickej-bezpecnosti.pdf

Public e-services

Quality and scope of public e-service		
Digital public services for citizens (0/2) **Criteria** At least 70% of services or information concerning service for citizens is provided online, and via a portal. Services that are offered fully, partially or not at all online.	Yes **No**	**Evidence** https://bit.ly/3jjYScS
Digital public services for businesses (2/2) **Criteria** At least 70% services or information concerning services for businesses is provided online, and via a portal. Services that are offered fully, partially or not at all online.	**Yes** No	**Evidence** https://bit.ly/3jjYScS
Pre-filled forms (0/2) **Criteria** At least 60% of data that is already known to public administrations is pre-filled in forms presented to the user	Yes **No**	**Evidence** https://bit.ly/3jjYScS
Individuals interacting online with public authorities (last 12 months) (0/2) **Criteria** Percentage of individuals who have used Internet, in the last 12 months, for interaction with public authorities exceeds 70%. It includes obtaining information from public authorities' web sites or downloading official forms or sending filled in forms.	Yes **No**	**Evidence** https://bit.ly/3jjYScS
Mobile friendliness (3/3) **Criteria**	**Yes** No	**Evidence** https://bit.ly/3jaJIGM

At least 70% of services are provided through a mobile-friendly interface, an interface that is responsive to the mobile device		
User support (3/3) **Criteria** At least 70% of online support, help features, and feedback mechanisms are available	**Yes** No	**Evidence** https://bit.ly/3jaJIGM
Proactivity		
Does the state request an input from the citizen before providing a service? (1/2)	Yes **Partially** No	**Evidence** https://www.mirri.gov.sk/aktuality/plan-obnovy-a-odolnosti/predstavujeme-viziu-dalsich-dvoch-zivotnych-situacii-privitame-vas-nazor/index.html
Does the government anticipate needs and automatically deliver services before they are demanded by the users? (0/2)	Yes Partially **No**	**Evidence**
Does the law require authorities to apply once only approach? (0/2)	Yes Partially **No**	**Evidence**