HUMAN RIGHTS IN AI-ENABLED E-GOVERNANCE: A COMPARATIVE STUDY OF KAZAKHSTAN AND ESTONIA

A THESIS

Presented to the MA Programme

of the OSCE Academy

in Partial Fulfillment of the Requirements for the Degree of

Master of Arts in Liberal Arts and Sciences with Specialization in Human Rights and Sustainability Programme

By Kristina Ryabova

January 2025

DECLARATION

Herewith I declare that I clearly understand §11 of the Academic Regulations and that the submitted paper is accepted by the OSCE Academy in Bishkek on the understanding that it is my own effort without falsification of any kind. I declare that I am aware of the consequences of plagiarism and/or cheating.

Kristina Ryabova

January 7, 2026

ABSTRACT

This MA thesis analyses the impact of AI-enabled e-governance on the realisation of human rights. For the analysis, I use the most similar system design model and examine two case studies – Estonia and Kazakhstan – during the period 2015–2025. Hereby, the analysis reflects the experiences of two countries with common ambitions, a comparable level of digitalisation, and a shared Soviet legacy, yet differing in their level of human rights protection. Therefore, it addresses emerging concerns about the misuse of AI technology by the state.

Therefore, I hypothesise that AI-enabled e-governance has an impact on the realisation of human rights (D.V.), and the extent of this influence depends on the state-related factors (I.Vs), such as international, regional and national legal frameworks, level of e-governance penetration, political will and political regime type.

To provide a more detailed and focused analysis, I concentrate on the health sector, which deals with highly sensitive data, with respect to such human rights as privacy, data protection and access to information, enshrined by Articles 17 and 19 of the ICCPR, Article 12 of the ICESCR, Article 8 of the ECHR, and Articles 7 and 8 of the EU Charter. Accordingly, my work responds to 2 main research questions: (1) what are the regulatory differences between the two countries regarding the protection of identified fundamental human rights and (2) to what extent the introduction of AI into e-governance systems affects the realisation of the human rights.

The comparative findings on Estonia and Kazakhstan demonstrate that AI-enabled e-governance does not impact the realisation of human rights by default. In contrast, it strengthens the existing political regime. The analysis shows a causal hierarchy in which political regime type is the decisive factor, as it shapes further regulatory adaptation. Another finding of my research is that e-governance penetration acts as an amplifier. In Estonia's democracy, it enables citizen control over personal data, but in Kazakhstan's authoritarian context, it expands state authority without proportional safeguards.

Finally, the study indicates that the influence of AI-enabled e-governance on human rights is not intrinsic, but instead stems from the existing governance context. In that way, the thesis addresses an existing gap in the literature by analysing the implications

of AI-enabled systems and tracing the connection between e-governance development and human rights, providing practical insights for governors and policymakers.

ACKNOWLEDGEMENTS

Dear reader,

This thesis is a result of a one-and-a-half-year journey. Many inspiring people supported me along the way, and I am grateful to all of you. If I did not mention your name here, please know that your help was important and highly valuable to me.

I would like to express my sincere gratitude to Dr. Anja Mihr for supervising and guiding me throughout this academic journey and creating the MAHRS program. Thank you for your support, care, and for sharing your time and experience with me, while leaving space for independent growth and development.

Special thanks go to my groupmates. We stayed connected throughout the whole program, and your insights helped me make important decisions that shaped the final version of this thesis. We faced challenges together and were looking for solutions together.

I would also like to highlight the important role of the entire OSCE Academy team. In particular, I am grateful to Dr. Pal Dunay for his leadership and wisdom in managing the institution, as well as to Aiym Chotoeva for her constant support, responsiveness, and assistance.

Last but not least, I am deeply grateful to my parents and friends, who supported me through this challenging period of academic and professional growth. Even being far from me in my home city of Almaty, your encouragement and belief made this journey possible.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

	International Human Rights Instruments
ECHR	European Convention on Human Rights
ICCPR	International Covenant on Civil and Political Rights
ICESCR	International Covenant on Economic, Social and Cultural Rights
UDHR	Universal Declaration of Human Rights
	Institutions and Bodies
CJEU	Court of Justice of the European Union
CIS	Commonwealth of Independent States
EAEU	Eurasian Economic Union
ECtHR	European Court of Human Rights
EDPS	European Data Protection Supervisor
EU	European Union
OECD	Organisation for Economic Co-operation and Development
ODIHR	Office for Democratic Institutions and Human Rights (OSCE)
OSCE	Organization for Security and Co-operation in Europe
UN	United Nations
	Concepts, Frameworks, and Methods
AI	Artificial Intelligence
D.V.	Dependent Variable
FATE	Fairness, Accountability, and Transparency
GDPR	General Data Protection Regulation
HRBA	Human Rights-Based Approach
I.V.	Independent Variable
ICT	Information and Communication Technology
ML	Machine Learning
M.V.	Meta Variable
MSSD	Most Similar Systems Design
PDPA	Personal Data Protection Act (Estonia)
	Governmental and Technical Terms
eID	electronic Identification
ENHIS	Estonian National Health Information System
G2B	Government-to-Business
G2C	Government-to-Citizen
G2G	Government-to-Government
KSI	Keyless Signature Infrastructure
TFEU	Treaty on the Functioning of the European Union
TTS	Transparency, Trust, and Security (Estonian governance principle)
	Indices and Measurements
EGDI	E-Government Development Index
GDI	Global Digitalization Index

CHAPTER 1. INTRODUCTION

1.1. Problem Statement and Hypothesis

As a main hypothesis for my thesis, I assume and argue that AI-enabled e-governance in Estonia and Kazakhstan has an impact on the realisation of human rights. Throughout the study, I focus on the public health sector over the ten years, from 2015 to 2025, to ensure a more focused analysis. This sector and time period were chosen as exemplary because the e-governance infrastructure in both countries was already well-established, and AI emerged as a technology that changed both legal and practical aspects.

The selection of countries also ensures the relevance of my research for stakeholders across several regions. In that sense, Estonia and Kazakhstan offer a valuable comparison due to their shared Soviet legacy, regional leadership in digital development, high levels of governmental digitalisation, and common political priorities. However, they diverge significantly in the protection of human rights and the regional regulatory frameworks governing e-governance with respect to the analysed human rights. Estonia is a party to several international and regional binding human rights instruments. In contrast, Kazakhstan pursues a more independent trajectory in introducing AI, prioritising national legislation and policy frameworks over its voluntary commitments to international human rights norms and other human rights instruments.

To enable a deeper analysis, the thesis focuses the (1) right to privacy and (2) the right to data protection and opposing them (3) the right to access to information as guaranteed by Articles 17 and 19 of ICCPR, Article 12 of UDHR, Article 8 of the ECHR, and Articles 7 and 8 of the EU Charter, and several other human rights instruments, which will be discussed in the following chapters. As well, the thesis focuses on the health sector, which involves especially sensitive forms of privacy due to the handling of personal medical data.[1]

[1] It should be noted that the introduction of AI in e-governance systems touches upon a wide range of other human rights and public sectors beyond the scope of this study.

Furthermore, I assume that the extent of this influence depends on state-related factors, such as existing e-governance regulations in domestic laws, state commitments vis-à-vis international and regional treaties, the level of e-governance penetration, the type of political regime, and the narrative of political will and national priorities.

The hypothesis led to the formulation of two research questions:

- What are the international, regional, and national (domestic) regulatory differences between Kazakhstan and Estonia regarding the protection of identified fundamental human rights – the right to privacy, the right to data protection, the right to access information – in AI-enabled e-governance?

- To what extent does the introduction of AI into e-governance systems affect the realisation of the right to privacy, data protection, and access to information, as enshrined in Articles 17 and 19 of the ICCPR, Article 12 of ICESCR, Article 8 of the ECHR, and Articles 7 and 8 of the EU Charter, in Kazakhstan and Estonia?

The study addresses an emerging gap in the analysis of AI's impact on the realisation of human rights. While the realisation of human rights is explicitly discussed in academic literature, as well as in relation to the development of e-governance systems, the introduction of AI is not yet thoroughly considered. The value of my research is in its contribution to understanding how various state-related factors influence the human rights implications of e-governance systems, particularly in the context of AI implementation. Considering the growing global reliance on AI-driven public sector systems, my findings could inform more balanced and rights-oriented AI governance frameworks.

1.2. Literature Review

AI-powered e-governance is a significant research topic among scholars due to rapid technological advancements and its impact on various sectors, including governance, ethics, human rights, and policymaking. While some authors focus on the economic benefits of the technology (Al-Besher and Kumar 2022, 3-4; Al-Ansi et al. 2024), others discuss the sensitivity of human rights in relation to AI (Karamagioli 2008; Abri et al. 2009, 3; Engelke 2020). This research field encompasses multiple directions, including

regulatory frameworks, ethical concerns, and societal implications, yet it remains underexplored.

First, literature is abundant on e-governance and e-government. However, these concepts are often used interchangeably (Bannister and Connolly 2012), which can lead to confusion. In this thesis, the focus is on e-governance, which encompasses e-government but is not limited to it.

E-governance has differing interpretations among scholars (Backus 2001) depending on the focus of the research (Grigalashvili 2022, 183-184), but commonly it could be defined as the use of ICT by the state to deliver public services, ensure compliance with state responsibilities, and protect human rights. The definition is not explicit, as some refer to e-governance as the use of ICTs to support democratic services and relationships among citizens (Dawes 2008; Ali 2023, 10-14). Still, e-governance might exacerbate the democratic deficit (Jan 2025, 113) and does not necessarily exist in democratic settings. Moreover, with the development of technologies, the concept broadened, resulting in a more complex definition that operationalises normative governance ideas and facilitates interactions across G2C, G2B, and G2G domains (Srinivas n.d). Consequently, e-governance refers to the use of ICT to deliver public services and ensure that the state complies with its obligations, including protection of human rights, but is not limited by commitment to democratic principles.

In contrast, e-government refers specifically to the use of ICT to deliver government services to citizens and businesses (United Nations n.d.). Based on that, in this work, I understand e-government as a digital infrastructure for governance that enhances service delivery, communication, and information exchange within and beyond the public sector. While e-government improves operational efficiency and service accessibility (Akman et al. 2005), it does not fully encompass the broader normative and governance dimensions captured by e-governance.

Focusing specifically on the introduction of AI into e-governance, the primary goal identified in the literature is to automate processes and reduce paperwork (Haughton and Barnes 2023; Androutsopoulou et al., 2019, 8). However, with the increasing interest in big data models, the role of AI expanded to risk prediction and forecasting (Janssen and Helbig 2018, 3; Margetts 2022). The authors note that application of AI

in e-governance has both benefits and drawbacks: the technology improves certain areas, but also poses potential risks to various human rights domains (Abri et al. 2009). They underscore the usefulness of AI in governance for detection, prediction, and data-driven decision-making (Margetts 2022). Nonetheless, there are concerns regarding AI's role in regulatory efforts, particularly in combating online harms and managing the influence of machine learning (ML).

Another significant concern regarding the impact of AI on governance and human rights is transparency. AI has the potential to reinforce existing biases in governmental decision-making processes and undermine fairness and accountability. Scholars emphasise the strong influence of AI on the public sector and national security, and show both its transformative potential and capacity to amplify systemic inequalities (ibid.; Engelke 2020).

The academic literature continues to lack attention on the impact of AI in e-governance systems concerning the realisation of human rights. Authors typically analyse the readiness of these systems for AI integration, but rather focus on technical aspects or conceptual proposals made by governments (Linis-Dinco 2024). The impact of e-governance on human rights is often assessed from a forecasting perspective through frameworks such as Human Rights-Based Approaches (HRBA) and Fairness, Accountability, and Transparency (FATE) (ibid.; Diya, 2025). Scholars argue that while these frameworks are widely recognised, there is no consensus on normative values, and they are exposed to being misused (ibid.). As a result, scholars advocate for AI governance to be grounded in international human rights principles while acknowledging the challenges posed by politicisation and the selective application of those.

Simultaneously, many states are developing AI governance policies to incorporate the technology into various aspects of public life. Regional approaches vary. For instance, in Asia, there is a trend to move from soft regulations to stricter ones (Xu et al. 2024, 275-277), while in Europe, both soft and hard regulations are recognised (Cancela-Outeda, 2024). Scholars suggest that AI governance in Asia is influenced by historical internet governance models, leading to diverse regulatory landscapes, while the EU is working on establishing a unified framework (ibid.).

Moreover, discussions about AI regulation and how governments manage these processes attracted the attention of international organisations. The United Nations (2024, 4-11) states the transformative potential of AI, but the concern about the risks associated with unregulated development remains (United Nations General Assembly 2023). Analysts emphasise the necessity for global AI governance to prevent an inequitable distribution of AI benefits and to address digital divides (ibid.). Despite the number of existing frameworks and guidelines, there is an absence of a truly global and comprehensive governance structure that adequately evaluates the impact of AI-enabled governance on the realisation of human rights.

The existing literature presents a wide range of perspectives on the application of AI in governance, illustrates differences in regulatory approaches and the effects of political will and other factors on their enforcement. However, the application of AI-enabled governance concerning human rights remains under-researched, and no concrete comparative studies have been conducted. Additionally, in-depth analyses of legal frameworks in the e-governance sector are limited. My research aims to fill these gaps through a comparative study of Kazakhstan and Estonia, representing Central Asia and Europe, respectively. The study analyses the impact of AI-enabled e-governance on the realisation of human rights, specifically focusing on the rights to privacy, data protection and access to information, to provide a more detailed analysis.

1.3. Key Concepts

Given the varying interpretations of human rights[2] (Costa Val Rodrigues 2023) and the rapidly evolving nature of AI, it is essential to discuss the key concept used throughout the thesis more precisely.

The right to access information in the health sector is defined as an individual's right to seek, receive, and share information related to health concerns, provided that such access does not jeopardise the confidentiality of personal data. This definition is based on Article 19(2) of the ICCPR (United Nations, General Assembly 1966a), which guarantees the right to receive and share information without borders, as well as Article

[2] In the scope of the thesis I focus on the definitions provided by International human rights bodies and their comments. However, the intepretation of human rights might differ across academic sources, medias and national legislation.

12 of the ICESCR (United Nations, General Assembly 1966b), which affirms that everyone has the right to the highest attainable standard of health. This right assumes the accessibility of health-related data, as explained by the UN Economic and Social Council in General Comment No. 14 (2000). The Comment highlights that access to health-related information is a fundamental aspect of the right to health and must be made available without discrimination to all individuals within a state's jurisdiction. In this context, "accessibility," which is a part of the right to the highest attainable standard of health, includes "information accessibility" as a critical aspect, alongside physical and economic access.

In this thesis, privacy rights and data protection are viewed as interconnected but ultimately recognised as distinct due to the specific regulations at regional and national levels (EDPS 2025). Both rights oppose the right to access information (Banisar 2011). Therefore, depending on the context, privacy may serve as an umbrella term for both the rights to privacy and data protection, unless stated otherwise.

For the purpose of this work, I define right to privacy as the right of individuals for protection from unlawful or arbitrary interference with their personal and family life, home, correspondence, honour, and reputation, which is based on Article 17 of ICCPR (United Nations, General Assembly 1966a) and further defined by UN Human Rights Committee in General Comment No. 16 (1988), as well as by Article 8 of the European Convention on Human Rights (Council of Europe 1950). However, as all individuals exist within society, privacy is necessarily relative and context-dependent. The concept encompasses multiple dimensions, including the right to be left alone, the right to be free from observation, and the ability to maintain control over one’s personal beliefs, identity, behaviour, and information (Cooley 1907; Fried 1968; Janis; Koops et al. 2017, 487–494). For this thesis, the concept of privacy is narrowed to issues within e-governance systems. This means that privacy is analysed primarily in relation to digital data processing, algorithmic decision-making, and the functioning of state-managed information systems, and other cases related to e-governance.

Additionally, I note that a crucial aspect of the right to privacy is the right to seek an effective remedy when violations occur, which is usually treated as a distinct human right: under Article 2(3) ICCPR, states are obliged to provide accessible, impartial, and timely mechanisms for individuals to challenge unlawful data collection, misuse, or

surveillance and to obtain adequate redress (United Nations, General Assembly 1966a). Accordingly, for this research, the right to privacy considers the existence of effective remedies and institutional accountability mechanisms in cases where privacy interference occurs, including those arising from the use of AI technologies.

Finally, the right to data protection is more specific and defined as the right of individuals to control their personal data, ensuring fair, secure, and lawful processing for legitimate purposes, with safeguards against unauthorized access, use, or disclosure, as well as the obligation of state take the necessary measures in its domestic law to give effect to the basic principles for data protection. Although none of the major international human rights treaties include protection of personal information as an aspect of the right to privacy ("Data Protection and Privacy" 2025), this definition is rooted in Article 8 of the Charter of Fundamental Rights (European Union 2007) and Article 4 of Convention 108+ (Council of Europe 1981).

Another complex term is "realisation of human rights", which I narrow down and define for this analysis. Generally, it refers to the process through which individuals and groups gain the power to fully enjoy their inherent rights as outlined in national laws and international instruments. For this thesis, the realisation of rights is understood progressively: states are obligated to achieve full realisation of these rights over time, based on available resources. This encompasses not only legal guarantees but also practical implementation and enforcement, ensuring that people genuinely experience the freedoms, protections, and entitlements promised by these rights.

1.4. Theoretical Framing and Methodology

In the scope of this thesis, the theoretical framing is based on the two main concepts in human rights discourse: (1) access as a human right to information in the health sector, for example each person has the right to know about his/her health situation and at the same time on (2) the human right to privacy and data protection of someone's individual health data.

First of all, Kohlberg's Theory of Moral Development framework is considered for this thesis. Since the thesis employs a comparative case methodology, the theory is essential for understanding why variables such as political will, strategic priorities, or political regime type might lead to differences in the realisation of the right to privacy in the

health sectors of Kazakhstan and Estonia. Kohlberg's theory identifies three levels of moral reasoning: Pre-conventional, Conventional, and Post-conventional morality (Kohlberg 1973). The theory posits that moral reasoning is a necessary but not sufficient condition for ethical behaviour, and it develops progressively. Each subsequent stage, such as the evolution of the e-governance system, should reflect a more sophisticated and adequate response to moral dilemmas than the previous one (ibid.). This framework helps explain how the moral reasoning and ethical decision-making processes of political actors and institutions, shaped by their level of moral development, can impact the enactment and enforcement of discussed human rights in AI-enabled e-governance systems.

The thesis also considers Elena Karahanna's Information Boundary Theory to analyse the differences in realisation levels between the human rights studied. The theory explores how individuals establish and manage boundaries around their personal health information in digital environments, particularly in relation to ML and AI models (Stanton 2003). This theory refers to the existing tension between the right to privacy and access to information, highlights individuals' preferences regarding control over access to their medical records and underscores the challenges of maintaining privacy in an era of pervasive digital connectivity.

The thesis employs a comparative case study methodology, specifically utilising the Most Similar Systems Design (MSSD) (see Figure 1). This approach is commonly applied for analysing cases that share structural similarities, but differ in key outcome variables. The similarities and variations between the selected countries provide an opportunity to investigate how similar technological developments can result in varying levels of human rights realisation, influenced by selected independent variables.

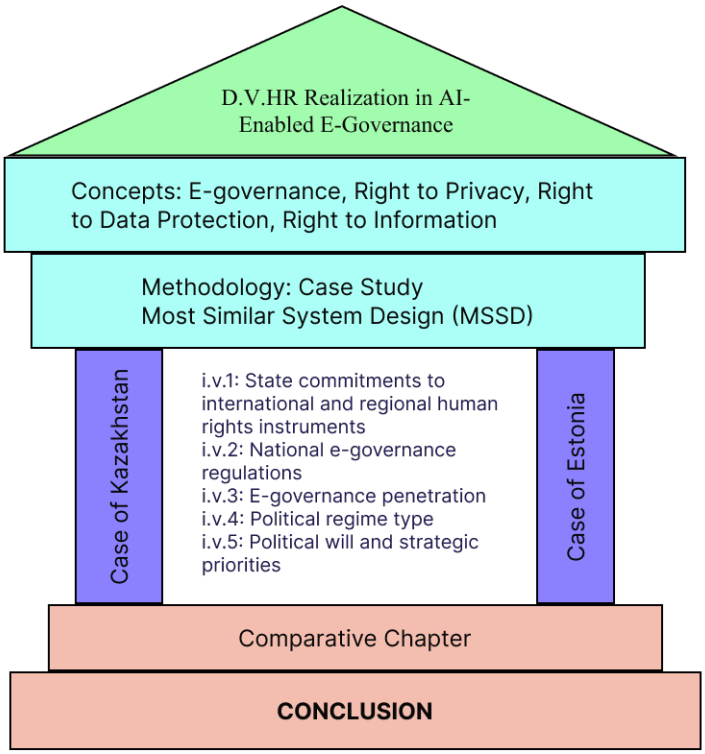

Figure 1. Greek temple design of the thesis. Source: created by the author

Kazakhstan and Estonia were selected as case studies because of their shared Soviet legacy, long-standing leadership in digital development within their respective regions, and high levels of government service digitalisation. Yet the countries differ in their records on human rights protection. According to the Global Digitalisation Index (SAMENA Telecommunications Council 2024), Estonia ranks 26th and Kazakhstan 58th, while in the E-Government Development Index (EGDI), they rank 2nd and 23rd, respectively (United Nations Department of Economic and Social Affairs n.d.). Moreover, both countries position themselves as leaders among post-Soviet states. At the same time, their Human Rights Index scores reveal a significant disparity in the level of human rights realisation (0.96 for Estonia and 0.53 for Kazakhstan) (Our World in Data 2025). This combination of similarities in digital advancement and differences in human rights performance makes the two countries particularly suitable for comparative analysis.

1.4.2. Research Model

The research model is built upon previously defined hypotheses and research questions. It assumes linear relationships between one dependent and five independent variables. The realisation of human rights is defined as the dependent

variable (D.V.), while various state-related factors are considered as independent variables (I.V.). The analytical framework is structured as presented in Table 1.

Table 1. Research Model

I.V.1: *State commitments to international and regional human rights instruments*	→	*D.V. HR Realisation in AI-Enabled E-Governance*
I.V.2: *National e-governance regulations*	→	
I.V.3: *E-governance penetration*	→	
I.V.4: *Political regime type*	→	
I.V.5: *Political will and strategic priorities*	→	

Source: created by the author

The independent variables were selected based on the description and discussion of e-governance models and their structural components presented in existing literature on the topic (Khalid 2016, 10-14; Dash and Pani 2016), and their interpretation was adopted for this research. Additionally, I consider the "People, Processes, Technology" framework, which is applied for digital transformation initiatives, including those that incorporate AI (Prosci 2025). In this context, the chosen variables not only reflect existing frameworks and concepts but are also reinterpreted and adapted to improve comparability with the goals of my research[3].

[3] Although the ultimate goal of the variables' selection is to provide an exhaustive and in-depth analysis of the impact of AI-enabled e-governance on human rights, the reader can also expect to find insights into the interconnections among them as part of the analysis. For example, the thesis addresses an ongoing discourse regarding whether political will can strengthen human rights safeguards (Brinkerhoff 2010; Beisheim et al. 2025) in the analysed sector or if these safeguards are ultimately shaped by the type of political regime. However, the thesis assumes political regime type as a default variable, and I do not aim to define it, but refer to the existing analyses. As well, the analysis assumes that political will and priorities for the AI integration in e-governance can both correlate and contradict with the political regime.

To ensure a clear and systematic comparative analysis, these variables are operationalised through both empirical and normative measurements (See Appendix A). The operationalisation for the systematic comparison of Estonia and Kazakhstan is presented in Table 2.

Table 2. Canva for the Systemic Comparison of the Findings

Case	I.V.1	I.V.2	I.V.3	I.V.4	I.V.5	D.V.	Discussion
Estonia							
Kazakhstan							
Source: Adapted from Carsten Ancker, "On the Applicability of the Most Similar Systems Design in Comparative Research," Journal of Social Research Methodology 11, no. 5 (2008): 398, https://doi.org/10.1036/3457041352.							

1.4.4. Scope of Data and Collection Methods

As previously mentioned, the analysis period is restricted to January 2015 through December 2025.[4] The analysis employs primary and secondary sources of qualitative data, along with secondary sources of quantitative data.

Regarding the primary sources, I focus on the texts of ratified international human rights instruments, regional treaties and conventions, national legislation, and other legal documents. I accessed these materials from the open databases such as Refworld, UN Treaty Bodies Database, EUR-lex, Riigi Teataja, Adilet and others. The sources of secondary data include, but are not limited to, comments on legal documents provided by official institutions, information available on state portals, news agencies, and even social networks, as state officials and experts often use these platforms as channels for public communication. Such statements were collected through open-source searches[5].

[4] It is important to note that as AI integration continues to evolve rapidly, the author revised the thesis chapters on national AI regulation multiple times. These revisions were driven by the introduction of new laws that directly relate to the main hypothesis. By the time the reader accesses this text, new amendments or changes may be introduced, which could cause some of the information contained herein to be less relevant.

[5] The author acknowledges that open search may have limitations and, technically, cannot cover all relevant information due to the specifics of web page indexing. As a result, certain pieces, such as statements from specific officials, might be absent in the analysis. However, the author made an effort to include the most significant information that has been widely discussed in the media or received particular attention from experts in the field.

Quantitative evidence was derived from international indices and datasets, including the UN EGDI, the Global Digitalization Index (GDI), the Human Rights Index, and regional indicators of internet penetration, digital literacy, and healthcare digitalisation. With that approach, I aim to ensure that the analysis captures not only normative obligations but also how they are interpreted, implemented, and reflected in practice. Moreover, to enhance the reliability and credibility of findings, I analyse the data sequentially for each country in Chapters 2 and 3, while the final chapter presents a cross-case comparison across the dependent and independent variables.

CHAPTER 2. WITHIN-CASE ANALYSIS – ESTONIA

2.1. Context: E-Governance and AI Development

The development of Estonia as a digital state must be understood in relation to its post-Soviet transformation and nation-building process. Following the collapse of the Soviet Union in 1991, Estonia emphasised a rapid digital transition as part of its political and economic reorientation toward liberal democracy and European integration (Björklund 2016, 914-924). Digitalisation was not only a technical modernisation project but also a symbolic reassertion of national sovereignty and independence.

From the late 1990s onwards, Estonia built a three-layered digital governance infrastructure: (1) the X-Road system of decentralised registries enabling secure data exchange between agencies, (2) a nationwide electronic identification (eID) system adopted by over 90% of the population, and (3) a service layer accessible through official portals such as eesti.ee (Margettsand 2017). These layers form the basis of Estonia's governance-as-a-platform model, which facilitates efficiency and transparency. These technological elements enable citizens to trace who accessed their personal data through audit trails, reinforcing accountability and trust in state institutions.

However, Estonia's digital transition also entailed significant rights trade-offs. The concentration of personal and public data in national databases meant that citizens accepted a reduced expectation of privacy in exchange for convenience and modernity (Björklund 2016; Randma-Liiv et al. 2025). Government strategies framed privacy less as an inherent citizenship right than as an issue of security and control. The Principles of Estonian Information Policy (1998) and

subsequent strategies, such as the Digital Agenda 2020 (2018), emphasised security and citizen "control over privacy" through technical safeguards, while acknowledging limited concern for privacy as a normative value. Scholars have observed that Estonians are uniquely willing to "sacrifice some privacy in exchange for efficiency" (Jackson, 2013, as cited in Björklund, 2016 922).

Initially, the compromise of privacy in favour of state democratisation was regarded as standard practice, and data protection was not prioritised. However, the cyberattacks of 2007 (Haataja 2018), then the largest of their kind against a sovereign state, marked a turning point, leading to the formal recognition of cybersecurity as a crucial human rights issue that directly threatens privacy. To safeguard this right, Estonia adopted several technical measures: the blockchain-based KSI technology was implemented to ensure the integrity of public records, and the world's first data embassy was established in Luxembourg to guarantee the continuity of digital services even under systemic threats (*Story - e-estonia* 2025; Espinosa and Pino 2024). These initiatives reinforced the principles of "transparency, trust, and security" (TTS), which scholars identify as the normative spine of Estonia's digital state (ibid.). However, they did not translate into greater citizen autonomy over personal data stored within government systems (ibid.).

AI integration since 2019 represents a continuation of Estonia's digital trajectory rather than a disruptive shift. The national AI strategy introduced regulatory clarity and a framework for embedding algorithmic tools into public services while upholding safeguards grounded in the TTS principles (*Story - e-estonia* 2025). Yet the realisation of human rights within this system sustained a central dilemma: should the right to privacy be exercised directly by citizens, or should it remain subject to governmental authority? In practice, blockchain and audit trails reframed privacy primarily as a technical matter of security rather than a substantive right of citizenship (Björklund 2016). The following chapters will examine how this tension plays out in the health sector, analysing the conditions under which the rights to privacy, data protection and access to information are realised in Estonia's AI-enabled e-governance.

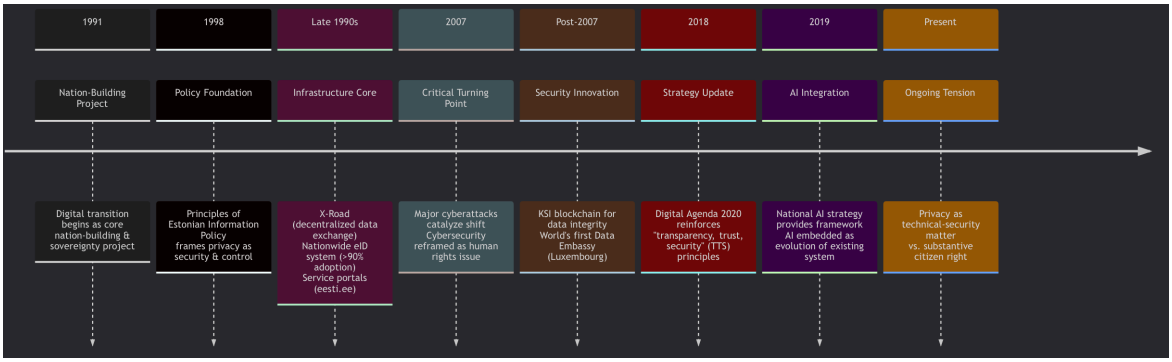

Figure 2. Timeline of Estonia's E-Governance and AI Development, 1990s–2025. Source: created by the author based on analysis of national strategies and laws. The timeline visualization was created with assistance from AI tools (DeepSeek).

2.2. Analysis of Independent Variables

2.2.1. State Commitments to International and Regional Human Rights Instruments

2.2.1.1 International instruments

The Estonian experience demonstrates that while international human rights instruments address privacy protection and information accessibility, their general provisions alone are insufficient to guarantee the realisation of human rights within the framework of an e-governance system. Although Estonia's e-governance system is influenced by its commitments to international human rights standards, reports from monitoring agencies reveal existing gaps in implementation practices and ongoing tensions related to the human rights discussed in the thesis.

In Estonia, access to information related to health is ensured by its commitments to Article 19 of the ICCPR and Article 12 of the ICESCR. While the ICCPR establishes a general framework for access to data, the ICESCR focus on this right in the health sector. However, it is important to note that, according to point 3 of Article 19 of the ICCPR, access to this information may be subject to legal restrictions. Based on the text of the document, these restrictions are necessary to respect the rights and reputations of others, protect national security, and maintain public order, health, or morals. Consequently, international commitments provide only a broad framework for data accessibility, allowing for restrictions at more detailed levels.

In terms of privacy, as a State Party to the ICCPR, Estonia is bound by Article 17, which prohibits arbitrary or unlawful interference with privacy and demands that any limitations must be lawful, legitimate, necessary, and proportionate. Similarly, Article

12 of UDHR safeguards individuals from arbitrary interference with privacy and is recognised as a norm of customary international law[6].

Estonia, in its Fourth Periodic Report to the Human Rights Committee (2018), stated that its legal framework for data storage and surveillance fully complies with Article 17 of the ICCPR and indicated that the country adheres to international human rights standards for privacy protection. In the report, the government emphasised the existence of extensive oversight mechanisms, which include prosecutors, courts, parliament, and the Chancellor of Justice; functioning of procedures for informing affected individuals; and the availability of legal remedies (ibid.). Furthermore, Estonia reported on its efforts to align its communication data regulations with evolving EU legislation and relevant statutes from the CJEU (ibid.).

Despite the commitments, the UN Human Rights Committee's Concluding Observations on Estonia's fourth periodic report (2019, para. 29-30) highlighted concerns regarding the compatibility of Estonia's processing and data retention practices with its obligations under Article 17 of the ICCPR. Specifically, the Committee criticised Article 111 of the Electronic Communications Act, which permits blanket retention of communications metadata. According to the concluding observations, this framework enables access to retained data not only for investigations of serious crimes but also for minor offences (ibid.). This raises questions about the necessity and proportionality of such measures with respect to international standards.

These issues have an ongoing nature. Although, by the same document from 2019, Estonia was recommended to ensure compliance with Article 17 and implement stronger safeguards against arbitrary interference by security and intelligence agencies, regulate the sharing of intelligence with foreign entities, and provide timely notifications and effective remedies, at the moment of observation, the author did not find specific amendments to the noted articles. Moreover, the Committee noted that these issues had been highlighted in the previous reporting cycle, with recommendations for Estonia to ensure legislative compliance with Article 17. The

[6] Importantly, as previously mentioned, the right to data protection is not explicitly defined in the major international human rights treaties. Consequently, on this level for Estonia, it could be interpreted only in relation to the right to privacy and insured by similar safeguards and normative regulations.

persistent nature of these concerns and the absence of relevant amendments to the specified article as of December 2025 indicate that Estonia's progress in balancing the efficiency of digital governance with the protection of privacy remains limited.

Focusing specifically on the health sector, Estonia faces challenges in balancing the rights to privacy and data protection with the right to access information. In its concluding observations on Estonia's third periodic report, the UN Economic and Social Council noted that many individuals living with HIV hesitate to seek antiretroviral treatment due to fears of stigma and the potential disclosure of confidential information to family members and employers (2019, para. 46). This raises concerns about the realisation of the right to privacy and data protection, as well as the state's ability to provide public health-related data while ensuring the right to information. Furthermore, in Estonia’s fourth periodic report under the ICESCR (2024), this issue is not addressed. However, it states that the protection of registry data is ensured through the assessment of availability, integrity, and confidentiality in line with the national information system security measures framework.

The analysis of Estonia's case highlights that the introduction of AI in e-governance systems poses new challenges to the realisation of human rights. The mere fact of international commitments ratification does not ensure effective protection of the discussed rights. Notably, AI-enabled e-governance is not specifically addressed in the existing ratified international documents and related reports. However, evidence suggests that the integration of AI technologies into Estonia's e-governance did not lead to measurable improvements or drawbacks in privacy safeguards and data protection practices. In contrast, unresolved issues such as blanket data retention and existing tensions between information accessibility and data privacy heighten the risks to the realisation of human rights in AI-enabled e-governance. With respect to the right to access the information, no related recommendations or information provided in state and civil society reports were observed.

2.2.1.1 Regional instruments

In the case of Estonia, regional regulation has a moderate influence over the realisation of the rights to privacy, data protection and information accessibility, establishing the principle of proportionality for the data regulation, supporting the rights realisation through regional institutions, but leaving the state power to set boundaries between

public and private benefits. Referring to the hypothesis, the thesis considers only a limited number of regional documents which have direct binding authority over Estonia as a Member State: Charter of Fundamental Rights of the EU (Articles 7, 8 and 11), TFEU (Articles 15 and 16), European Convention on Human Rights (Article 8), European Convention 108 and GDPR.

The right to privacy is ensured by Article 7 of the Charter of Fundamental Rights of the European Union, which guarantees individuals the right to respect for their private and family life (European Union 2007). However, Article 8 of the European Convention on Human Rights further defines the limitations on the realisation of the right to privacy, stating that interference can be lawful and necessary for reasons such as national security, public safety, the economic well-being of the country, the prevention of disorder or crime, the protection of health or morals, or the protection of the rights and freedoms of others (ibid.).

The practical limitations of the right to privacy are confirmed by regional human rights institutions such as the ECHR and the CJEU. A precedential case in this context is a case of Liblik and Others against Estonia, in which the ECHR confirmed that Estonia violated the right to privacy (European Court of Human Rights 2019). The Court found that placing the applicants under surveillance without sufficient justification in the authorisation decisions violated Article 8 of the European Convention on Human Rights (ibid.).

Additionally, the CJEU, in its judgment on a request from Estonia in November 2021, emphasised the necessity for the country to provide sufficient justification for interfering in private life (2021). The CJEU stressed the existence of national legislation that allows the public prosecutor’s office to authorise public authorities' access to traffic data, which by definition can include private calls and emails (ibid.). In that context, the precluding notion of the national legislation is seen as one heightening the risk for the analysed human rights.

In contrast to the international human rights instruments on the regional level, the right to data protection is defined as a specific right. It leads to a higher potential of its realisation in an AI-enabled e-governance structure. In the EU, the right to data protection is ensured by Article 8 of the Charter of Fundamental Rights of the EU. The

article specifies that everyone has the right to the protection of the personal data concerning him/her, as well as to the fair processing, accessibility and rectification of such (European Union 2007). Further, building on this basis, the GDPR and Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data serve as the legal instruments that regulate data identification and processing aspects.

Still, the regional framework for data protection has limits. According to Article 16 of GDPR, the framework does not address data protection issues which fall outside the scope of Union law, such as activities concerning national security. At the same time, its text emphasises the intent to harmonise the protection of fundamental rights with the free flow of personal data between Member States (European Union 2016). In other words, the GDPR recognises that the realisation of the right to data protection is not absolute and must be balanced according to the principle of proportionality but gives states flexibility in determining the scope of data processing depending on political will and priorities.

Importantly, GDPR provides a concrete definition of the health-related private data, which increases the potential for the realisation of the right to data protection in the health sector. Article 35 of GDPR defines Personal data concerning health should include all data about the health status of a data subject, which reveals information relating to the past, current or future physical or mental health status of the data subject (ibid.). This includes information about the collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU, such as an information derived from the testing or examination of a body, including from genetic data and biological samples, and any information on, for example, a disease, disability, medical history, and other (European Union 2011).

Article 53 of GDPR further distinguishes between general personal data and special categories of personal data, setting stronger safeguards on the latter (European Union 2016). According to that, special categories, such as health data, which is highly relevant to this thesis's focus on AI in e-governance, must be processed only when necessary to achieve legitimate purposes that benefit individuals and society. These purposes include managing health or social care services, public interest archiving, scientific research, and health system supervision.

Another pillar of the regional data protection framework is Convention 108, which regulates the processing of data and is acknowledged as the first internationally recognised document that addresses the issue. This convention outlines the responsibilities and duties of Estonia as a state party (Article 4) to recognise the right to privacy while reaffirming the freedom of information, as stated in the preamble (Council of Europe 1981).

The right to information, which is opposed to the rights to privacy and data protection in the scope of this thesis, is governed by the already discussed documents. Specifically, it is ensured by Article 15 of the TFEU. This article grants any natural or legal person the right to access documents held by the Union's institutions (Conference of the Representatives of the Governments of the Member States 2012). Additionally, Article 4 of Convention 108+ also addresses this right.

As of 2025, the author did not find any recorded cases related to the violations of the right to privacy, data protection, or access to information in the health sector in Estonia. However, concerns about potential risks to these rights remain, as there are ongoing cases in other public sectors. One case is referred to as Case 3-22-1148, which the Supreme Court of Estonia submitted to the CJEU on March 21, 2025. This case involves an individual's request to the Money Laundering Reporting Bureau for information concerning suspected money laundering, which was denied (Dataguidance, 2025). The Supreme Court is questioning whether national laws can limit the rights of data subjects as outlined in Article 23 of the GDPR. As of December 2025, the case is ongoing.

In May 2019, the government of Estonia signed the OECD Principles on AI (Grigoryan 2019). These principles emphasise human-centric and ethical AI development, in line with the EU approach and the recommendations provided by the OECD in their Recommendation of the Council on Artificial Intelligence (OECD 2019). Based on that and according to Article 1.2 of this document, Estonia is committed to respecting privacy throughout the AI system lifecycle (ibid.). Additionally, Article 2.1 ensures that the government respects privacy and data protection while supporting the environment and development of AI (ibid.). In other words, Estonia's commitment to this document highlights its voluntary compliance with upholding human rights.

The regional legal framework in which Estonia operates provides safeguards for the realisation of the right to privacy, data protection, and data access in AI-enabled e-governance. Moreover, this framework not only addresses traditional forms of governance but also recognises e-governance as a distinct issue. However, the scope of its regulation is limited to the mandates of the Union's law. With this in mind and reflecting on the hypothesis, Estonia's regional commitments moderately influence the realisation of the analysed rights. Although these commitments establish a complex framework that recognises and addresses specific human rights, they also authorise the state to override those rights in circumstances not addressed by Union law.

2.2.1.3. National e-governance regulations in Estonia

Estonia’s national regulation has the most decisive influence over the realisation of human rights compared to international and regional frameworks, due to its direct application and evolving nature with respect to the introduction of new technologies in e-government systems. Estonia’s national e-governance framework operationalises its international and regional commitments, but also complements them and specifies the conditions and limitations for the realisation of the right to privacy and data protection and access to information.

The foundation lies in the Constitution of the Republic of Estonia, where §26 guarantees the inviolability of private and family life, §43 protects the confidentiality of communications and §44 ensures free access to information disseminated for public use (Republic of Estonia 2025). Consequently, all of the analysed human rights are recognised on the constitutional level separately, which provides a normative basis for their realisation.

Further, the right to privacy is protected under Articles 137, 156, 157, and 157-1 of the Estonian Penal Code. These articles establish penalties and fines for violating the right to privacy, including unlawful access to and disclosure of private information (Republic of Estonia 2015). Article 157 extends the protection of the right to privacy in the context of professional activities, while Article 157-1 introduces higher fines for the disclosure of sensitive data, including health information (Republic of Estonia 2015). These regulations have general provisions and are not specific to any public sector, making them universally applicable. This universality permits them to adapt to evolving forms of governance, such as those enabled by artificial intelligence. However, the official

statistics do not reflect the application of these articles, which might indicate both the absence of related cases or the absence of complaints and non-disclosure.

Focusing on data protection, the core of Estonia's data protection regime is the Personal Data Protection Act (PDPA), which transposes the GDPR into domestic law and establishes the principles governing the processing of personal data, but at the same time, it specifies conditions under which the personal data can be used without informed consent. For instance, Article 6, point 1 of PDPA specifies that personal data may be processed without consent for the purposes of scientific and historical research or official statistics (Republic of Estonia 2019). The data should be pseudonymised for these purposes. However, point 2 of the same article allows depseudonymisation for the needs of additional research, in line with point 1 of the article (Republic of Estonia 2019).

PDPA and Penal Code legitimise processing of medical data for specified public health purposes such as research, occupational medicine, or threat management without prior informed consent of the subject matter, if it adheres to necessity and proportionality principles (Republic of Estonia 2019). This aligns with GDPR and is transposed via PDPA §6, allowing authorised personnel (e.g., health professionals) to access and analyse pseudonymised health data for e-governance functions. Moreover, AI-driven diagnostics can be conducted without risking criminal liability under Penal Code §158, as long as there is no unauthorised leakage of health data (Republic of Estonia 2015). Additionally, depseudonymization is permitted when necessary for further data processing, provided there is a public interest, and the obligations of the data subject remain unchanged (Republic of Estonia 2015).

Focusing more on the digital forms of medical data, in the health sector, privacy and data processing regulations are outlined in the Health Services Organisation Act and related regulations, which establish stricter rules for managing sensitive health data. Under these regulations, medical information is stored centrally on the national e-Health platform and can be accessed by authorised professionals for legitimate purposes without the permission of the data subject (Republic of Estonia 2018). According to Article 59-3(3) of the Health Services Organisation Act, patients have the right to prohibit access to their health data in the Estonian National Health Information System (ENHIS).

The national legal framework includes an opt-out mechanism that allows patients to restrict access to their health records. However, at the state level, there is a legal toolkit for the usage and processing of health data. This means that data processing can occur without patient consent unless the patient actively chooses to opt out. Consequently, the combination of technical limitations, existing legal flexibility, and potential unawareness among citizens regarding their options to limit access to their personal records increases the risks to privacy and data protection in AI-enabled governance.

The right to access personal health information is realised through the centralised state portal, terviseportaal.ee. The right to access personal health data is mainly governed by Article 59-3 of the Health Service Organisation Act. This article guarantees that patients have access to their personal data in the Health Information System (Republic of Estonia 2018). However, it also permits healthcare providers to impose a time limit on when this information can be forwarded to the information system, during which individuals can only examine their medical records through a healthcare professional. The underlying reason for keeping this limiting provision is the acute risk of self-harm. However, the law does not specify the conditions or time limits for setting these limits, which contradicts the intention of ensuring access to information.

Referring to the main hypothesis of the thesis, the combination of national laws and policies creates a complex regulatory framework, but in the context of AI-enabled e-governance, existing legal flexibility heightens the potential risks for privacy and data protection. AI technologies enable fast and extensive data processing, which can shift the burden of safeguarding against data breaches and unauthorised disclosures from individuals to the state and service providers. While Estonia's regulatory framework grants individuals control mechanisms such as the right to prohibit access to health data and to monitor who accesses their records, the rapid and automated nature of AI-driven data processing may worsen vulnerabilities.

Concerning the right to information, AI-enabled e-governance has a dual effect. Positively, AI improves the processing of health-related information at scale and speed, service delivery and enables more transparent, algorithm-based reasoning for regulating access to sensitive data. For example, AI facilitates faster assessments on whether access requests meet legal criteria for disclosure. Negatively, inaccuracies or

biases in AI algorithms may cause delays or false denials in information access, potentially infringing on the right to access information.

Therefore, Estonia's national regulation illustrates that while AI-enabled e-governance offers significant benefits for fulfilling public health objectives and the right to information, it imposes new risks to privacy and data protection that require further adoption of governance frameworks.

2.2.3. E-governance Penetration

In Estonia, the increasing use of AI-enabled e-governance systems is somewhat limiting the realisation of the right to privacy and data protection, while having a moderate positive impact on the right to access to information. Individuals lack alternatives for storing and managing their data, despite having tools to control it. Since the public sector is nearly fully digitalised, any attempt to access a service involves sharing data with public institutions.

In 2024, EGDI score of 0.9727, a substantial increase from 0.85 in 2018, following the implementation of its AI strategy in 2019 (Invest Estonia 2024). This score ranks Estonia second globally, and indicates that e-government, as a digital tool of e-governance, is developing substantially and increasing the e-governance capacity. The index evaluates three main pillars: human capital (digital literacy), telecommunication infrastructure, and the quality and accessibility of online services, although it does not assess human rights compliance separately. Nevertheless, the evaluation of technical aspects indicates improved accessibility to services, which leads to a higher potential for the realisation of human rights. Estonia has nearly fully digitalised its services, receiving outstanding scores in user support (98/100), user data control (87/100, significantly higher than the EU average of 65), and mobile accessibility (97/100) (e-Estonia 2021). This digital infrastructure facilitates broad and effective citizen engagement with e-governance platforms.

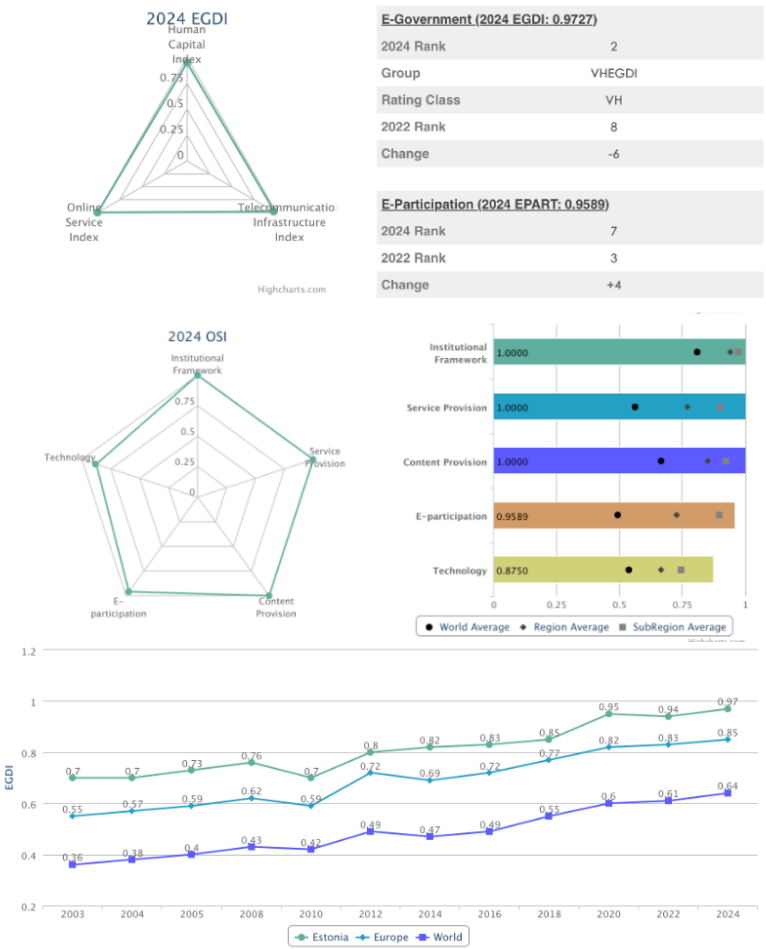

Figure 3. EGDI for Estonia. Source: UN DESA DPIDG 2025

In the context of pervasive e-governance penetration, the health sector demonstrates both the efficiencies and human rights challenges of digitalisation. Estonia's national e-Health system is progressive: 99% of patients' digital health records are accessible countrywide, and 100% of prescriptions are issued digitally (e-Estonia 2025). The system presents extensive use: the doctors submit about 2.5 million queries, and patients approximately 2.7 million monthly through the e-Health portal (e-Estonia 2025).

This concentration of sensitive health data within a centralised digital system accelerates healthcare delivery and enables integration of AI tools for diagnosis and personalised medicine. However, it simultaneously exposes patients to heightened privacy risks (Conduah et al. 2025), as the scale and speed of AI-enabled data processing increase the potential for unauthorised profiling, data breaches, and non-transparent decision-making.

Estonian systems are performing quite effectively when it comes to the right to access information. As of 2025, 97.5% of Estonians have access to their electronic health records, significantly surpassing the EU average of 79.1% (Republic of Estonia, Ministry of Justice and Digital Affairs 2025). Citizens can fully access all their electronic health data, including medical images in digital format, through the browser version of the national e-health platform, which is mobile-responsive. This access is enabled by a national online service using eID authentication. According to state reports, the data is updated following each healthcare encounter, and real-time remote assistance is available in case of any issues (e-Estonia 2025).

As of 2025, AI and ML technologies have been integrated into e-governance systems, including healthcare. Big data and data science are utilised for optimising processes, analysing resource usage, validating analytical results, and providing tools for the independent verification of certificates (Republic of Estonia, Ministry of Justice and Digital Affairs 2025). AI-enabled e-governance is also interconnected with the Internet of Smart Things, bringing about changes in processes and influencing people's daily behaviours, particularly regarding health data. Consequently, the integration of new technological solutions into existing e-governance structures positively impacts the realisation of the right to access information by simplifying data access processes, increasing the operational productivity of e-governance systems, and enabling quicker access to health information.

In the existing e-governance structure, citizens primarily rely on legal safeguards for the realisation of their right to privacy and data protection and procedural controls within the platform, including the ability to monitor access logs, deny visibility to specific providers, and restrict data sharing for research. However, these controls operate within a framework where complete exclusion from data inclusion is nearly impossible. This reality makes robust legal enforcement and institutional accountability essential for protecting privacy. On the other hand, the right to access health-related information has been positively enhanced by technological advancements, which facilitate easy and timely access to this information.

These findings highlight the core hypothesis: the level of e-governance penetration with respect to AI integration shapes human rights realisation by making data inclusion universal, privacy and data protection dependent on the quality of governance and

increasing the realisation of the right to access information by ensuring faster delivery. Estonia demonstrates that while digital public services offer immense benefits and accessibility, ensuring the right to privacy demands ongoing regulatory adaptation and political will to address emerging AI-related risks effectively.

2.2.4. Political Regime Type

The democratic nature of Estonia's political regime plays a decisive role in ensuring the realisation of human rights, particularly the right to privacy, data protection and access to information. In a liberal democracy such as Estonia, privacy and transparency are both a politically and instrumentally justified value, grounded in democratic principles of autonomy and individual freedom (Lever 2006). According to Freedom House (n.d.), Estonia functions as a liberal democracy, while the V-Dem Institute (n.d.) classifies it as a consolidated democracy. Both organisations emphasise the strength of Estonia's institutional safeguards and the effectiveness of its human rights protection mechanisms. These assessments indicate that Estonia's political regime not only formally guarantees but also actively facilitates the realisation of privacy rights through transparent governance, judicial independence, and strong accountability structures. In this context, the democratic regime serves as a fundamental condition enabling the protection and practical realisation of human rights.

Freedom House specifically evaluates the judicial framework and independence as part of its overall assessment. According to 2024 data, Estonia scored 6.5 out of 7.0 in this category (Freedom House 2024). The report indicates that the judicial framework has not experienced significant changes since 2016, which was before the introduction of AI in governance. However, the Delivery Portal, launched in 2022, according to them, enhances the transfer of documents between administrative and judicial bodies, thereby reducing errors and delays in handling cases.

Data from V-Dem shows that the political regime ensures the realisation of the right to privacy through the established legal safeguards. It assesses the degree to which the legal framework restricts government access to personal data online, using a scale from 0 to 4, where a score of 4 indicates that access is permitted only under extraordinary circumstances (V-Dem Institute n.d.). Estonia achieved a score of 3.9, demonstrating a strong level of explicit safeguards for privacy.

While privacy and data protection and access to information in the health sector are not evaluated separately, it can be concluded from these assessments that the indices do not indicate a negative impact of AI-enabled e-governance on the realisation of analysed human rights due to strong adherence to the good governance principles; rather, it is likely to benefit from it.

2.2.5. Political Will and Priorities

Estonia's political will and strategic priorities positively correlate with the realisation of the right to privacy, data protection and access to information, as it is framed as an ambition to be a global benchmark in digital governance. This results in significant investments in e-governance and AI technologies, a strong commitment to transparency and human rights principles at both national and international levels.

Estonia's government frames its digital transformation as a tool to not only improve governance efficiency but also to uphold privacy protections and human rights (Espinosa and Pino 2024; Republic of Estonia, MEAC 2021). The Ministry of Economic Affairs and Communications articulates this vision through an action plan aimed at the widespread adoption of AI solutions across public and private sectors by 2030. The government has committed €85 million to implement this strategy, which includes investments in the development of AI and data management systems, as outlined in the White Paper on Data and Artificial Intelligence for 2024–2030 (Err, 2024). This policy framework defines strategic objectives to build a strong data economy, a citizen-oriented AI ecosystem, and a digital state based on transparency, accountability, and human-centric governance (Kratid n.d.).

At the same time, in the political context, Estonia continues to pursue digitalisation as a key element that distinguishes it from other post-Soviet states. Estonia's geopolitical realities – particularly its proximity and historically complex relationship with Russia – reinforce the strategic importance of using smart, data-driven technologies to safeguard national sovereignty and strengthen societal resilience. As Estonia's ambassador to the U.S. aptly stated, "Whatever we lack in size, we can compensate for by using data smarter" (Vincent 2025). In this sense, maintaining the image of a digitally driven democracy serves not only as a technological goal but also as a component of Estonia's political identity and independence.

Estonia's commitment is also manifested in high transparency standards and active international engagement through education and collaboration initiatives. The government openly shares best practices and supports capacity-building for colleagues from other countries, signalling its leadership role in the global digital governance ecosystem (e-Estonia 2024).

However, the political will has imbalances with respect to the right to privacy and data protection. Critiques have arisen concerning Estonia's data retention laws that grant extensive access to personal data by state agencies, raising concerns about privacy and the potential for overreach, as political intentions are supposed to be balanced with legal safeguards (Estonian Human Rights Centre 2017). In the context, this imbalance shows that political will is inclined to focus less on ensuring the right to privacy, while still enabling the right to access information by investing in infrastructure development.

2.3. Impact of AI-enabled E-governance on the Realisation of Human Rights in Estonia

Referring to the hypothesis, the analysis reveals that in Estonia, AI-enabled e-governance has a neutral impact on the realisation of privacy and data protection rights, while enhancing the right to access information, particularly in the health sector.

Despite technical advancements and governmental commitments, privacy violations within Estonia's e-health system occur, often exacerbated by data centralisation. Recent incidents highlight these vulnerabilities. In 2024, personal and health data of approximately 10,000 individuals were illegally accessed from the genetic testing company Asper Biogene's database (ERR News 2023). In 2025, a vulnerability in the data protection system of Allium UPI OÜ, which manages Apotheka's loyalty program, compromised the privacy of over 750,000 customers. This breach resulted in repeated unauthorised data downloads and led to a €3 million fine imposed by the Data Protection Inspectorate (ERR News 2024). However, as previously defined, the author considers the right to privacy and data protection realised if legal remedies are effectively enforced. In other words, despite these recorded violations, adherence to established legal procedures and enforcement mechanisms demonstrates the functioning realisation of the right to privacy and data protection in practice.

With respect to access to information, cases referring to its violation were not found in the judicial records and news. While, as previously noted, accessibility of information is technically enhanced by AI-enabled e-governance.

The analysis of Estonia emphasises that AI-enabled e-governance has an impact on the realisation of human rights with respect to the discussed variables. However, the flexibility of legal frameworks across different levels indicates a higher importance of other variables, such as political will and regime type. At the same time, a gradual transition from physical services to digital services, and then to proactive digital services enhanced by AI (FedScoop 2025) has a higher positive impact on the right to access information, while privacy is impacted neutrally. This experience supports the hypothesis that there is a relation between AI-enabled e-governance and the realisation of human rights, and state-related factors determine whether AI in e-governance strengthens or undermines the right to privacy.

CHAPTER 3. WITHIN-CASE ANALYSIS – KAZAKHSTAN

3.1. Context: AI-Enabled E-Governance Development

In Kazakhstan, the introduction of e-governance and AI in the system was primarily a response to changing global digital trends and administrative needs, rather than a proactive, strategic initiative based on a comprehensive human rights framework. This led to a reactive approach to regulating the e-governance sector and a lack of effective regulation at the initial stages. Additionally, the regulation and implementation of e-governance were inconsistent, resulting in a fragmented set of laws and policies that did not always address a specific issue, being narrow in scope of regulation.

The first steps towards the widespread adoption of ICT in general and in health care specifically began in the 90s of the 20th century with the introduction of basic information systems aimed at the formation of aggregated (not personalised) databases, mainly for state statistics (Ministry of Healthcare of the Republic of Kazakhstan 2020). In the early 2000s, the Ministry of Healthcare developed a set of registers to collect data on the medical care provided to people with certain types of diseases, such as chronic renal failure, diabetes, tuberculosis, etc (ibid.). However, the first legislative step towards digital governance came later in 2003 with the Law “On Electronic Document and Electronic Digital Signature”. The law laid foundational legal

recognition for electronic identification mechanisms, essential for later e-government services.

In 2006, the official launch of the eGov.kz marked the formal introduction of e-governance. Initially, it served as an informational platform (Haidar 2025). In the health sector, elements of digital governance were introduced similarly in 2006 when the national project "Unified Health Information System" was launched (Republic of Kazakhstan 2004). Under this project, the Ministry of Healthcare created a software that provided functions to automate all the main functions in the healthcare system, from collecting medical data at the level of healthcare providers to monitoring the quality of medical services at the level of the national agency responsible for this function. However, soon the enforcement of the project was delayed beyond the originally planned deadlines and by 2012, the project was cancelled due to technological and conceptual obstacles (Ministry of Healthcare of the Republic of Kazakhstan 2020).

Later in 2013, Kazakhstan attempted to renovate the e-governance sector again with the state program called "Informational Kazakhstan 2020". It set the eHealth development strategy for 2013-2020 in Kazakhstan (ibid.). One of the goals of the program was to create a centralised system of healthcare, which would allow citizens to get all the services, from making an appointment to full access to the medical data digitally. At the same time, the regulation of data processing and ensuring the security of data was not yet fully developed, and still relied on the legislation coming from 2003.

Additionally, in 2017, the Kazakhstani government launched the national "Digital Kazakhstan" program. While the program aimed to institutionalise the digital transformation agenda, its objectives did not directly target the realisation of human rights but focused primarily on modernising public administration, improving electronic document management, and strengthening cybersecurity frameworks (Republic of Kazakhstan 2017).

Subsequently, in 2024, Kazakhstan approved the Concept for the Development of Artificial Intelligence for 2024–2029. Although this concept referred to the European Union's regulations as exemplars of legal safeguards for human rights realisation, it

explicitly stated that existing regulations and normative acts would suffice to ensure these protections (Republic of Kazakhstan 2024).

As a result, Kazakhstan has implemented several programs and strategies aimed at maximising the benefits of digitalisation. However, these initiatives have often prioritised technological advancement and sectoral development over placing citizens' rights and protections at the forefront of the digital transformation agenda. As of December 2025, a new law on artificial intelligence was accepted, notably after the deployment of AI-assisted tools in government services and various sectors. This regulatory delay raises concerns about the protection and realisation of privacy rights, data protection and access to information, especially considering the sensitive nature of health data processed within e-governance systems (OECD 2022).

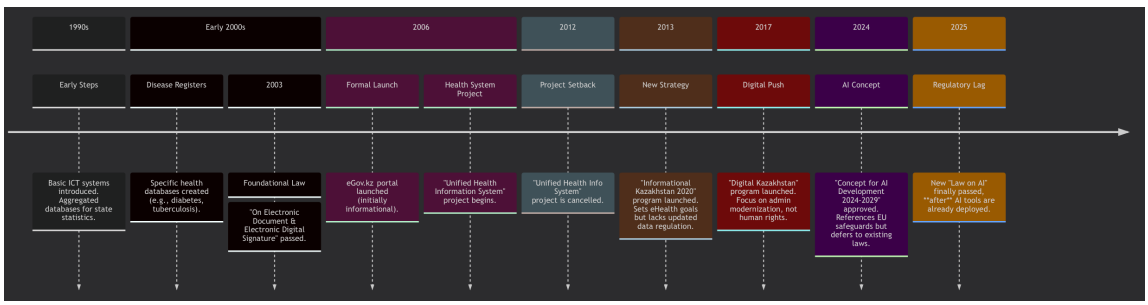

Figure 4. Timeline of Kazakhstan's E-Governance and AI Development, 1990s–2025. Source: created by the author based on analysis of national strategies and laws. The timeline visualization was created with assistance from AI tools (DeepSeek).

3.2. Analysis of Independent Variables

3.2.1. State Commitments to International and Regional Human Rights Instruments

3.2.1.1. International instruments

Kazakhstan is a party to key international human rights instruments that guarantee the right to privacy, data protection and access to information. Particularly, the state ratified ICCPR, which enshrines this right to privacy and data protection in Article 17 and recognises the right to access the information by Article 19, ICESCR, which confirms the right to access health information by Article 12 and recognises the principles of the UDHR as customary law. Further, in 2018, Kazakhstan expressed interest in ratification of the Convention 108 to commit internationally to the protection of data (Ius Laboris 2024). However, the mere fact of ratification of these treaties and the intention to ratify international conventions does not ensure the realisation of the human rights analysed in this thesis.

There is a reported low level of realisation of the right to privacy, data protection and access to information, according to both international institutions and local NGOs. In its Concluding Observations on Kazakhstan's third periodic report for September 2025, the UN HRC (2025) specifically urged the State to adopt comprehensive legal and procedural safeguards to prevent the misuse of surveillance powers to ensure the realisation of the human rights guaranteed by Article 17 (para. 50) and to ensure access to information held by public bodies (para.10) as defined in Article 19 of ICCPR. This criticism aligns with concerns raised by Kazakhstani NGOs, which report that national courts often permit limitations on the right to privacy and data protection, referring to the need to balance individual rights with the interests of society and the State, a concept interpreted broadly as the "public interest" (Civil society report to UN HRC 2025a).

Submissions from NGOs and expert analyses highlight the incompatibility of the existing legal framework with the country's international obligations under Articles 17 and 19 of the ICCPR. Reports indicate that since 2013, the Law on Personal Data and Its Protection has regulated the handling of personal information (Civil society report to UN HRC 2025b, para. 30). According to the reports, the underlying reason is the fragmentation of the legal landscape. Additionally, reports indicate limited sectoral protections outlined in the Labour Code and the Law on Informatisation and in the Law on Access to Information (2015). The latest, for instance, permits limitations on access only as specified by other legislation and to the extent necessary to protect the constitutional order, public order, the rights and freedoms of others, and public health and morality.

In its opinion on Kazakhstan's request for accession to Convention 108 from October 2018, the Consultative Committee emphasised that the current national legislation governing data protection rights does not align with the provisions of the convention and needs to be revised (Council of Europe 2018). Specifically concerning the health sector, the Committee pointed out that the absence of provisions defining and establishing appropriate additional safeguards for special categories of personal data, in accordance with Article 6 of Convention 108, represents a significant weakness in the law (ibid.). As of December 2025, the analysis by the thesis author did not reveal amendments to the indicated legal acts.

Therefore, simply ratifying major international human rights instruments, along with a stated intention to ratify additional ones, does not automatically result in a higher level of realisation of the rights to privacy, data protection, and access to information. While ratifying treaties establishes a state's obligations under international law, it does not ensure their effective incorporation into domestic legislation, and thus the realisation of human rights. However, international instruments still have a positive impact on the realisation of human rights, as they provide an independent international record of breaches of these rights.

3.2.1.2. Regional instruments

Regional instruments have a formal impact on the realisation of the right to privacy in Kazakhstan, due to their non-binding, recommendatory nature. Kazakhstan is not a party to any binding regional treaties specifically dedicated to privacy rights, data processing or access to information. However, as a member of regional organisations such as the Organization for Security and Co-operation in Europe (OSCE) and the Eurasian Economic Union (EAEU), Kazakhstan is subject to policy frameworks and recommendations that indirectly influence the discussed human rights.

Within the OSCE framework, Kazakhstan reaffirms its commitment to key OSCE human rights principles, including privacy, data protection and access to information. Nevertheless, monitoring reports highlight gaps in compliance with OSCE standards in areas related to privacy. For example, a trial monitoring report published in May 2025 by OSCE experts indicated that the mobile phone numbers of participants in trials conducted via WhatsApp were not sufficiently safeguarded (OSCE/ODIHR 2025, para. 250). While this issue is not directly linked to the central hypothesis of this study, it reflects the broader perception of privacy protection by state authorities.

EAEU influences Kazakhstan’s data governance and protection primarily through its regulatory framework, addressing consumer protection, data transfers, and economic transactions within the Union[7]. However, these efforts did not end in binding regulations. Further, in December 2020, the EAEU adopted the Strategy for Development until 2025, aiming to create a unified digital space regulated by an

[7] The Union regulation is structured around the economic aspects, rather than data of individuals. The mentioned regulations do not directly refer to the main hypothesis but is mentioned a one of the elements of the regional data processing structure.

internal treaty on data turnover (EEC 2020). In 2021, initial steps were taken to regulate cross-border data transfers among EAEU member states. Despite these ambitions, by 2025, no formal document has been signed or ratified. As a result, the EAEU currently lacks specific binding norms addressing data protection and health data, therefore, or establishing comprehensive e-governance frameworks, resulting in its influence on Kazakhstan's data protection landscape being largely advisory.

In parallel, discussions on AI regulation took place at the Commonwealth of Independent States (CIS) level. The development of a model law on artificial intelligence technologies was expected to be completed in 2025, potentially providing some harmonised standards for the region (ECCIS 2024). Yet, as of December 2025, the absence of binding regional instruments continues to characterise Kazakhstan's regulatory environment.

In summary, Kazakhstan's regional commitments through organisations like the OSCE, EAEU, and CIS primarily provide normative frameworks and technical guidance that inform the country's approach to privacy, data protection and information accessibility in AI-enabled e-governance. Due to the non-binding nature of these instruments and limited enforcement mechanisms, however, the realisation of human rights rests mainly on Kazakhstan's domestic legal framework and maintained governance principles.

3.2.2. National E-governance Regulations

In Kazakhstan, the realisation of the rights to privacy, data protection and access to information, both generally and within the health sector, relies predominantly on domestic legal regulation, which remains the primary binding mechanism governing state obligations. Still, domestic regulation does not ensure the full realisation of the discussed rights even in formal settings, as it presents significant terminological and formulation gaps (Akhmetova 2023; Abdrassulova and Kostyanaya 2025, 37-38).

The Constitution of the Republic of Kazakhstan, as the supreme legal document, reflects the state's formal obligations under international treaties. Article 18(1)– (2) of the Constitution guarantees the inviolability of private and family life, as well as the privacy of correspondence and communications. The same article also ensures the right to access information, obliging state bodies, public associations, and officials to provide every citizen with the opportunity to become acquainted with information concerning

their rights and interests[8] (Republic of Kazakhstan 1995). However, Article 39 explicitly permits limitations on the exercise of these rights by law and to the extent necessary to protect the constitutional system, public order, human rights and freedoms, or the health and morals of the population[9] (ibid.).

The regulation of privacy and data protection within Kazakhstan's e- governance framework is defined by the Law on Personal Data and Their Protection (2013). According to Article 2, the law's purpose is to "ensure the protection of the rights and freedoms of a person and citizen upon collection and processing of personal data (Republic of Kazakhstan 2013). While this establishes a nominal legal safeguard, the law's numerous exceptions substantially weaken its protective capacity.

First, according to Article 1-12 of the Law, the definition "processing of the personal data" does not consider its collection (ibid.). In other words, the Law considers fragmented regulation of different procedures related to data. The fragmentation itself does not impose risks on the realisation of the right to data protection. However, the Law does not explicitly note that all the processes related to data, including its collection, should align with the human rights safeguards.

Secondly, Article 9 of the Law authorises the collection and processing of personal data without consent in several circumstances, including law enforcement operations, statistical activities, and the implementation of international treaties (ibid.). These exceptions create loopholes through which personal data, especially in state-administered digital systems, can be processed without explicit individual consent. As such, the law constructs a conditional rather than absolute right to privacy, subordinating individual autonomy to institutional and administrative interests.

Further Article 7-7 of the Law on Personal Data and Their protection provides very general provisions on the collection of data in electronic information resources, which

[8] Importantly, this covers both publicly available information and personal information with limited access. Consequently, it quarantines the right of an individual to access his/her private stored data, including data related to health (Commentary on Article 18 2025).

[9] In Kazakhstan, Article 4 of the Constitution states that ratified international treaties take priority over domestic laws (Republic of Kazakhstan 1995). This enables citizens to refer to these treaties when national laws do not offer sufficient protection in national courts. Additionally, citizens can submit complaints to the international treaty bodies, provided that relevant protocols for individual communications are ratified.

lack sufficient clarity. It states that the specifics of collection and processing in such electronic systems "shall be specified by the legislation of the Republic of Kazakhstan on informatisation" (ibid.). However, the law does not directly reference which provisions of that "informatisation" legislation apply, nor does it mandate any concrete standards or procedures. As a result, the regulation of data collection in electronic information resources remains ambiguous and under-defined.

Additional constraints arise within the public administration domain, where data integration for public services is regulated by Article 8-1 of the same law (ibid.). This article requires compliance with legal provisions on various forms of confidential information, specifically state, commercial, and family secrets. Yet it omits medical data from explicit classification. This reflects an institutional prioritisation of administrative efficiency over the sensitivity of personal health information.

The handling of medical data is instead governed by the Code on Public Health and the Healthcare System, defined by Article 57 (Republic of Kazakhstan 2020). These include the digitalisation of healthcare data and processes, the establishment of technical standards, and the protection of healthcare information systems containing personal data. The Code also guarantees patients access to their data and emphasises confidentiality. However, it simultaneously states that the collection, processing, and storage of personal health data form part of the provision of medical services - implying that consent to treatment is treated as implicit consent to data processing. Consequently, patients have limited control in determining how their health data is used within Kazakhstan's e-health system.

The right to access to information in Kazakhstan is regulated by a separate Law on Access to Information, which does not explicitly secure access to medical records. Despite the right being guaranteed by the state and formalised in Article 1(2) of the Constitution (Republic of Kazakhstan 2015), the law sets specific conditions for accessing certain types of public health information, such as data on the health situation, sanitation, and demography owned by authorities. Those, according to Article 6, cannot be subject to limitations, but at the same time, the law does not guarantee access to personal medical records (ibid.). Consequently, there is a strong statutory emphasis on public health data, while at the individual level, the right to access one's own medical records is not explicitly secured.

Accepted in November 2025, the Law on AI was expected to have a positive impact on the existing legal framework for the realisation of the right to privacy, data protection and access to information. However, it largely refers to the existing regulations. For instance, Articles 10 and 11 of the Law on AI guarantee the realisation of the rights on privacy and data protection in relation to the application and usage of AI, but these human rights are guaranteed in compliance with already existing regulations, gaps of which were discussed previously (Republic of Kazakhstan 2025).

Importantly, according to Article 12, the state is responsible for carrying out its functions under the Constitution of the Republic of Kazakhstan as well as other existing regulations, including those in the sphere of AI (ibid.). In other words, the law confirms the state's obligation to comply with norms safeguarding the analysed human rights in the context of AI-enabled e-governance. Still, the text does not specifically address the inclusion of AI in e-governance systems as a distinct regulatory subject. It also overlooks important aspects such as access to information, transparency of algorithms, and the use of training data. Additionally, it does not focus on particular sectors, such as healthcare.

This legal architecture demonstrates that Kazakhstan's framework for privacy, data protection and information accessibility, though extensive in formal provisions, remains state-centric in practice. Analysed human rights are safeguarded primarily insofar as they align with state and institutional priorities, particularly administrative digitalisation and public sector efficiency. This confirms the hypothesis of this study: in Kazakhstan, the realisation of human rights within AI-enabled e-governance is impacted by AI-enabled e-governance and conditioned by the nature of state regulation and political will, which privilege control and administrative functionality.

3.2.3. E-governance Penetration

In Kazakhstan, the growing penetration of AI-enabled e-government services presents implications for the realisation of the right to privacy and data protection, while it enables the right to access to information. Although e-government coverage is not yet universal, allowing many citizens to access most services in person and thus be more directly aware of when and how they share their data, this flexibility does not fully extend to the health sector. In healthcare practice, the ability to withhold personal data is often limited, as data is frequently entered into centralised systems automatically,

often without the informed consent or awareness of citizens and lacking proper control mechanisms. Still, it allows them to access personal health records more efficiently.

Kazakhstan's digital transformation is reflected in its EGDI, which rose to 0.9009 in 2024, a significant increase from 0.725 in 2016 following the introduction of the Digital Kazakhstan program (UN DESA DPIDG 2025). Of the three pillars comprising the EGDI, the country performed best in the Online Services Index (0.939), while the Human Capital Index (0.84) reveals persistent challenges in adult literacy and educational attainment (ibid.).

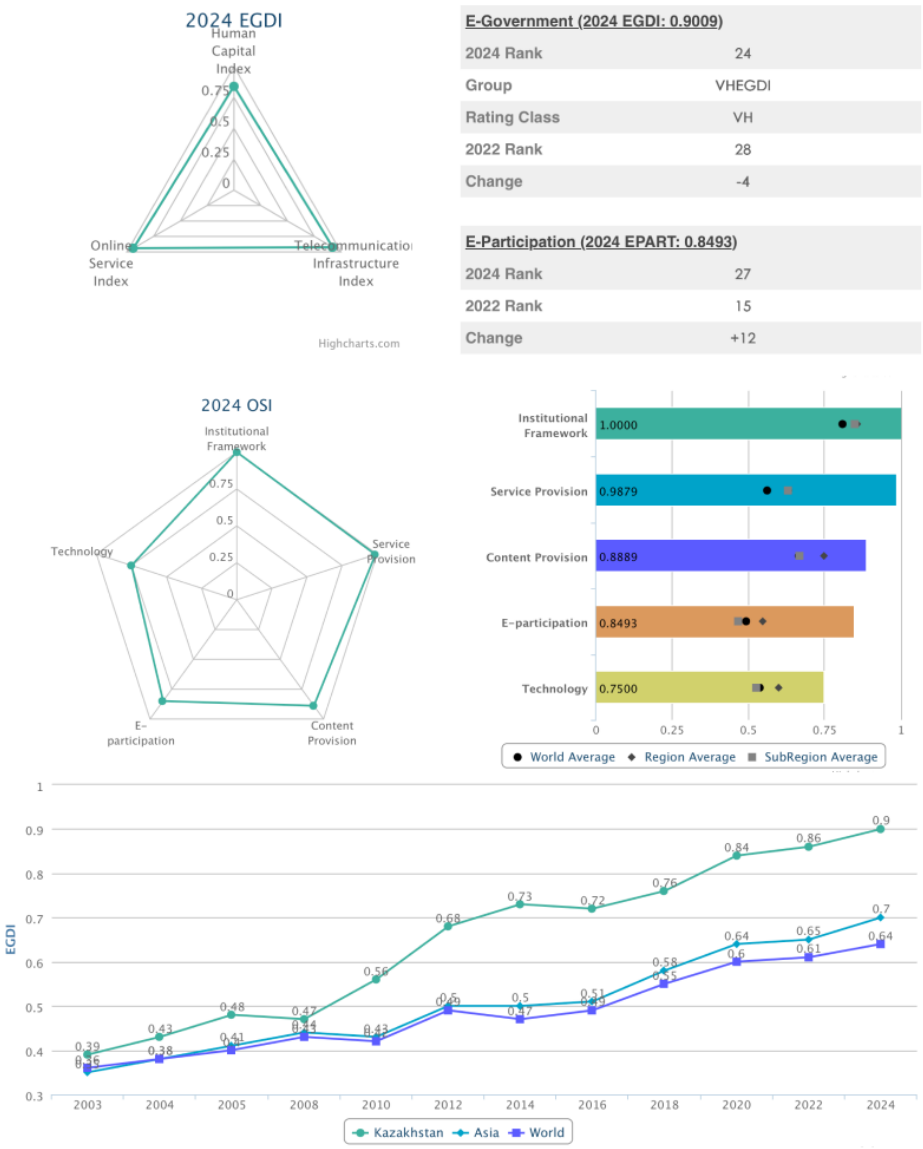

Figure 5. EGDI for Kazakhstan. Source: UN DESA DPIDG 2025

By the end of 2025, 15.1 million users were registered in the e-government system, out of a total population of 20.9 million (MAIDD 2025). As of 2025, over 92% of government services were accessible online, and 90% are available via mobile applications (Prime Minister of the Republic of Kazakhstan 2025).

Digital health sector penetration parallels this growth: by late 2025, data for 80% of citizens is integrated into centralised storage (Inform-Kazakhstan 2025). Currently, health information systems, such as the most used one, Damumed, accumulate health data regardless of whether citizens have directly opted in, since healthcare providers are mandated to record each patient interaction and enter personal health data in the system by default. The introduction of the national E-Densaulyq platform is scheduled for launch in 2026[10] (ibid.).

In terms of access to health information, this right is similarly processed through the health information systems, such as Damumed, E-clinic, InfomedKazakhstan, etc. (RCEZ 2025). Based on the description provided by one of the operators, the system enables access to a wide range of information related to the public medical services (Damumed n.d.). Through the application or platform, an individual can access his/her medical records, results of medical tests and check-ups, comments of specialists and information on free medical services available. In addition, the platform provides information on schedules and availability of specialists and the story of medical insurance payments. Access to the information is regulated and ensured by a user agreement and has both free and paid features[11].

Despite this rapid digitalisation, Kazakhstan's current e-governance has not effectively translated into stronger protections for privacy, data protection or information accessibility. The volume of personal data in the centralised digital health systems grows, but individuals lack technical and legal control over their personal information and are often unaware of their profiles and their content within these platforms. Moreover, under the current regulation, operational realities and gaps in technical safeguards are often undermined. Moreover, the data is often stored on the servers of

[10] As of December 2025, no official follow-up was found.
[11] The integration of the third party within the system partially moves the responsibility for data accessibility, as additional inter-party regulation is introduced, and formally, the government cannot intervene in this relationship.

private companies, so its protection and accessibility are regulated and ensured by them, and the state has only limited control over it.

Consequently, AI-enabled e-governance penetration in Kazakhstan has a moderate impact on the realisation of the rights to privacy and data protection, as individuals still retain the technical opportunity to avoid digital systems and not share their health data. However, it significantly affects the right to access information: if an individual uses authorised e-health platforms, they may gain access to a wide range of their personal medical information. In this way, the level of e-governance penetration has a neutral impact on the realisation of the right to privacy and data protection, but a moderately positive impact on the realisation of the right to information, though that impact still entails inherent risks introduced by third-party involvement in the system.

3.2.4. Political Regime Type

In the case of Kazakhstan, the political regime limits the realisation of the analysed rights due to an imbalance of power between institutions and the robust legal frameworks. Freedom House (2025) characterises Kazakhstan as a consolidated authoritarian regime, in which executive dominance shapes policy outcomes. In 2025, assessments indicated that Parliament functions mainly as a procedural body that approves executive initiatives with minimal debate, while judicial oversight of executive power remains limited (Freedom House 2025). Within such a governance structure, the introduction of AI into public administration heightens risks to privacy and other fundamental rights, as policy decisions involving algorithmic tools can be implemented with little transparency and accountability.

Under current regulatory conditions, the judiciary is widely regarded as institutionally weak and susceptible to executive influence. Freedom House scores Kazakhstan around 1.25 out of 7 on indicators of judicial independence and protection of civil liberties (ibid.), revealing systemic deficiencies in due process and access to remedies for rights violations. These gaps are particularly significant when digital governance systems rely on automated decision-making, data collection, and algorithmic profiling, as affected individuals have limited recourse to challenge potentially unlawful or discriminatory administrative actions. As well, it applies to the right to access to information, as a lack of transparency and absence of legal tools leads to conditions for the violation of the right.

The V-Dem (n.d.) dataset scores Kazakhstan 1.4 out of 4 in the privacy domain, placing it in a range associated with extensive government access to personal data and limited individual safeguards. The absence of independent oversight mechanisms, such as a data protection authority or parliamentary committees dedicated to digital rights, further amplifies vulnerabilities.

Taken together, these indicators define a political environment in which AI-enabled e-governance carries significant risks for the realisation of privacy rights, data protection and information access, including in the health sector. The horizontal integration of AI across public services, data registries, and decision-making processes occurs within a political and legal architecture that offers minimal insulation against rights erosion.

3.2.5. Political Will and Strategic Priorities

Kazakhstan's political leadership demonstrates strong intentions to introduce AI across the majority of governmental processes. This commitment is consistently reflected in national policy documents and public statements of officials, revealing a state-driven ambition to embed AI into all spheres of public administration. The declared objectives are twofold: increasing bureaucratic efficiency and strengthening citizens' trust in state institutions through automation and digital transparency (Prime Minister of the Republic of Kazakhstan 2024; President of the Republic of Kazakhstan 2024).

In 2024, the government initiated a nationwide audit of state functions as a preparatory stage for AI integration. According to Vice Minister of Artificial Intelligence and Digital Development Dmitry Mun, approximately 40,000 state functions were reviewed to identify those most suitable for automation with minimal risk (Profit.kz 2025). This process includes the Ministry of National Economy and the Ministry of Finance to create a unified registry of state functions, identifying areas where AI can have the greatest administrative impact. Such systematisation represents an noteworthy centralisation of administrative data and decision-making capacities under algorithmic systems, signalling the government's preference for efficiency-oriented technological transformation over participatory or rights-based digital reforms.

The political narrative around AI integration emphasises national progress, transparency, and data security, yet omits specific commitments to enhancing human rights safeguards. Galymzhan Koishybayev, Head of the Prime Minister's Office,

highlighted that the government "will continue to actively work on implementing artificial intelligence in all spheres of life," with a focus on "data security and compliance with legislative norms" (Prime Minister of the Republic of Kazakhstan 2024). The same discourse frames AI primarily as an economic and governance tool rather than as a potential challenge to privacy or accountability. The official rhetoric of "transparency and efficiency" therefore grows within a technocratic paradigm that assumes legal compliance as sufficient for rights protection, without addressing the substantive realisation of the right to privacy. Still, conceptually, it positively references the realisation of the right to access information, as AI-enabled e-governance is presumed to enhance transparency and optimise data collection practices. However, it remains unclear in current discourse whether individuals are considered the primary beneficiaries of improved information accessibility or if the focus is primarily on increasing the efficiency of government processes.

President Kassym-Jomart Tokayev's 2024 address further institutionalised this orientation by mandating that every new public service must be created digitally "from the outset," and that once data is provided to the state, it "should not be requested again" (KT.kz 2024). Interpreting the term, the data introduced to any of the government systems once is supposed to be available in all other by default. Additionally, he proposed that all normative acts governing interactions between citizens and the state should undergo mandatory "digital expertise" prior to approval (ibid.). While these initiatives aim to streamline bureaucratic procedures and eliminate redundancy, they also consolidate data flows and expand state control over personal information. On the other hand, this priority ensures that individuals would be able to access their data through any government platform with equal ease, while the corresponding data control mechanisms, such as consent management, data correction, and deletion, remain undiscussed.

The health sector illustrates the practical application of these strategic priorities. Deputy Prime Minister and Minister of Artificial Intelligence and Digital Development, Zhaslan Madiev, announced that a key milestone in the digital transformation of healthcare will be the launch of the Unified State Medical Information System (Profit.kz 2025b). This system will integrate AI tools such as the "AI-therapist" for preliminary diagnosis generation, an agent for identifying anomalies in laboratory

analyses, and an agent for verifying the justification of medical services (ibid.). These innovations promise improved diagnostic accuracy and service efficiency, and positively impact the right to access to information.

From the perspective of this thesis's hypothesis, Kazakhstan's political priorities reveal a clear pattern: the state's AI agenda is driven predominantly by the pursuit of administrative efficiency and technological advancement rather than by the enhancement of human rights realisation. While official documents refer to "data security" and "legal compliance," they lack explicit provisions for strengthening privacy, data protection, independent oversight, or public participation with respect to AI deployment. It indicates that current political priorities reflect the political regime, and state representatives do not change the narrative to recognise the right to access personal medical information, although AI-enabled governance, according to them, should improve transparency of the systems.

3.3. Impact of AI-enabled E-governance on the Realisation of Human Rights in Kazakhstan

In Kazakhstan, the introduction of AI-enabled e-governance resulted in a higher risk for the realisation of the right to privacy and data protection, particularly within the health sector. The elevated privacy risks can be attributed to several factors, including weaknesses in national legislation, political priorities that emphasise technical aspects over individual rights, and the absence of robust and systematic control over e-government services. The right to access data benefits from AI-enabled e-governance, but only to the extent that it aligns with the interests of the third-party operators that manage Kazakhstan's e-health system and is more driven by market demands. Consequently, Kazakhstan's international and regional commitments offer some moderation of these risks, but significant gaps in domestic legislation persist, creating spaces where violations of the right to privacy can occur.

Recent incidents involving health data breaches illustrate these concerns. In August 2024, personal medical records of first- to fourth-year female students from Al-Farabi Kazakh National University located in Almaty were leaked. The documents, which contained names, individual identification numbers, phone numbers, and sensitive gynaecological information, were publicly shared on social media. According to official accounts, the breach resulted from an error by a nurse employed by a private

company providing medical services to the university; this nurse sent the students' documents in Excel format via WhatsApp to a specialist in the dean's office, who then shared them in the public chats (Kursiv Media 2024).

Similarly, in April 2025, another privacy breach was reported involving the unauthorised disclosure of HIV status data belonging to individuals at a college. The leaked dataset contained personalised information, confirmed by screenshots shared in the media. However, state representatives disputed the authenticity of this case (Kursiv Media 2025).

In both cases, details regarding subsequent legal proceedings or remedial actions were not made publicly available, raising concerns about the effectiveness of remedy mechanisms intended to restore the right to privacy. Moreover, the scale and nature of these breaches indicate that privacy and data protection in Kazakhstan are not strictly enforced, as multiple specialists involved in data handling had access to sensitive information. These incidents support the principal hypothesis of this thesis, demonstrating that, in Kazakhstan, human rights related to privacy and data protection within AI-enabled e-governance initiatives are more threatened than realised. In contrast, the information accessibility is increased, according to state officials (El.kz 2025; Prime Minister of the Republic of Kazakhstan 2023), while no cases of violations were found in open sources.

CHAPTER 4. COMPARATIVE ANALYSIS AND DISCUSSION

4.1. Systematic Comparison of Findings

In this chapter, I move from within-case examination to an explanatory comparative analysis. The following sections conduct a systematic, variable-by-variable comparison, assessing differences and similarities in how each independent variable shaped the dependent variable – the realisation of the right to privacy in AI-enabled e-governance. The comparison identifies the differing significance of the analysed independent variables and shows that in the analysed cases, the political regime played a role of meta-variable, and political priorities were reflected in that, which led to the catalysing nature of AI-enabled e-governance with respect to the analysed human rights.

4.1.1. Comparative Analysis of Independent Variables

4.1.1.1. State commitments to international and regional human rights instruments

The analysis of state commitments reveals an architectural difference between Estonia and Kazakhstan: the presence or absence of a binding regional legal order. This difference moderates the effectiveness of international human rights law in shaping domestic practice for privacy, data protection, and access to information. Estonia's human rights framework is characterised by its integration into the European Union's legal framework, which enforces its international treaty obligations and provides regional instruments for human rights protection. In contrast, Kazakhstan's engagement with the international human rights system is extensive on paper, but lacks binding enforcement mechanisms.

Referring to the initial operationalisation of variables, the thesis reveals that the primary divergence is not the fact of ratification, but the enforcement system. For Estonia, the EU provides a supranational enforcement mechanism (CJEU, GDPR fines, ECtHR) that actively interprets and compels compliance, bridging the gap between international norms and domestic law. For Kazakhstan, the absence of such a mechanism means international and regional commitments stay in the domain of diplomacy and soft power, easily overseen by domestic political priorities and offering citizens no direct legal alternative based on supra-national law. Therefore, while both states are formally committed to similar international standards, the realisation of privacy, data protection, and access to information is far more contingent and constrained by regional binding law in Estonia, and highly dependent on domestic political will in Kazakhstan.

When examining the impact of the variable across the analysed rights, it is noteworthy that cases and violations of the rights to privacy and data protection are more prevalent than violations of the right to access information in reports from international and regional human rights institutions. This suggests that AI-enabled e-governance has a more negative effect on the realisation of the right to privacy and the right to data protection than on the right to access information. However, it is important to note that remedies are still available, which contribute to the realisation of these rights.

In the context of the hypothesis, the results indicate that the existence of binding regional frameworks for AI-enabled E-governance leads to stronger safeguards, while

ratification status does not ultimately result in a higher level of the realisation of human rights.

4.1.2. National E-governance Regulations

The analysis of national regulations demonstrates a significant impact on the realisation of human rights. The differences in the level of human rights realisation in AI-enabled e-governance systems across different national legal frameworks can be explained by the contrasting regulatory philosophies of Estonia and Kazakhstan[12]. Estonia adopts a citizen-centric, rights-oriented model, while Kazakhstan follows a state-centric, efficiency-focused model. This fundamental distinction directly influences how rights such as privacy, data protection, and access to information are articulated and defined within legal norms.

Estonia's domestic legal framework is coherent, detailed, and built with adaptability that allows it to integrate international and EU norms more efficiently. Additionally, the Estonian system emphasises citizen control, supported both technically and legally by the state. In this context, while data processing for healthcare can proceed based on implied consent, the legal framework provides individuals with the tools needed to protect and safeguard their privacy and data. Furthermore, the legal right to access health-related information is guaranteed and ensured through government platforms. In that way, Estonia's e-governance regulatory approach is not static, ensures adherence to the fundamental rights by default, and easily adapts to the new technological advancements, such as AI.

Kazakhstan's regulatory landscape, while extensive in volume, is characterised by internal fragmentation, omissions, and permissive exceptions that systematically prioritise administrative functionality over individual rights. The Constitution of Kazakhstan guarantees the right to privacy and access to information, but it also provides a limitation clause, allowing rights to be restricted by law, which sets rights as conditional. Other legal acts do not resolve the issue, as they do not fully capture the data processing cycle. Specifically in the health sector, the Code on Public Health treats

[12] From the author's perspective, the evolving nature of national AI regulation can be influenced by the prevailing philosophy of the political regime or specific political priorities within a particular sector. However, as will be discussed in more detail further in the analysed cases, national regulation correlates with the political regime and the national priorities.

consent to medical treatment as implicit consent to data processing, while there is no statutory equivalent to Estonia's opt-out mechanism. In that context, the 2025 Law on Artificial Intelligence references existing law and enforces existing gaps, rather than introducing new safeguards.

Finally, the core difference between the two frameworks lies in their regulatory approaches and the ultimate purpose of the law. Estonia's framework is designed to empower individuals by providing clear, actionable tools, such as opt-out options, logs, and sanctions. In contrast, Kazakhstan's framework is focused on efficient administration and offers flexibility for the state through exemptions and limitation clauses. This approach acknowledges that national courts possess the highest authority in legal matters to collect, process, and use data with minimal need for individual consent. As a result, in Estonia, the rights to privacy, data protection, and access to information are active and exercisable claims. In Kazakhstan, however, these rights are largely passive and vulnerable, which heightens risks in AI-enabled systems.

4.1.3. E-governance Penetration

The analysis of e-governance penetration demonstrates that while high levels of digitalisation are present in both cases, its impact on the realisation of human rights is not uniform but is instead moderated by the nature of the governance system. Referring to the hypothesis, the e-governance penetration shapes rights outcomes by making data inclusion universal, which negatively impacts the right to privacy and data protection, where the degree can be controlled by the introduction of technical safeguards, and positively impacts the right to access health information.

In Estonia, the deep integration of digital services creates an environment where high penetration is integrated with control tools and technical safeguards, enabling the realisation of the right to privacy. At the same time, universal digitisation of health records does not risk data protection rights by utilising architectural features of the e-health system and provides citizens with direct access to their personal health information. The introduction of AI into this ecosystem acts as an integrative layer, enhancing access to information through faster data processing. While centralisation creates targets for breaches, the remedy mechanisms show effectiveness, which is one of the defined conditions for the right realisation.

Conversely, in Kazakhstan, high penetration is seen as widespread digital inclusion without corresponding citizen agency or state-guaranteed safeguards. Digital engagement is extensive but often passive, as data entry is frequently automatic and mandated for service providers. This structurally undermines the realisation of the rights to privacy and data protection. The right to access health information is facilitated through third-party platforms and user agreements, not enshrined as a state-guaranteed entitlement. The deployment of AI-enabled tools into this architecture is lacking technical consent mechanisms, independent oversight, and citizen control features. The documented health data breaches show how high penetration increases exposure to harm without strengthening protective structures.

The comparative analysis highlights that e-governance serves as a governance amplifier. Estonia's rights-based democracy enhances empowerment, transparency, and accessibility. Conversely, in Kazakhstan's state-centric system, it increases data collection capacity and control, which raises concerns about privacy and data protection while providing a tenuous form of information access. This illustrates that the impact of e-governance is not determined solely by technology; rather, it is influenced by the existing political and regulatory environment into which AI is implemented.

4.1.4. Political Regime Type

The relationship between the political regime and human rights realisation is not linear, contrary to what the initial model suggested. In the process of data analysis, I found that regime type was the primary factor explaining the different paths in the realisation of human rights, more so than other variables. In relation to various arguments and instances of rights violations previously discussed, the political regime can be viewed as a meta-variable that establishes general patterns for other factors in AI-enabled e-governance in both situations. It shows that in AI-enabled e-governance systems, democracy institutionalises constraints on power that promote rights protection, whereas authoritarianism tends to concentrate power, creating inherent risks to human rights.

In Estonia, the consolidated liberal democracy provides the essential infrastructure for the realisation of privacy, data protection, and access to information. This ensures that legal norms are not formal but enforceable and create a system of horizontal accountability. Consequently, institutions like the Data Protection Inspectorate and the

Chancellor of Justice can function with independence, and citizens have credible avenues for legal challenge and remedy.

In Kazakhstan, the consolidated authoritarian regime creates a political environment where power is vertically concentrated, and individual rights are subordinate to state interests. Within this framework, privacy, data protection, and access to information are not viewed as inherent checks on power but as potential barriers to state control, public order, and administrative efficiency. In that way, the authoritarian regime thus generates a vicious cycle: it fosters political will focused on control and efficiency, produces state-centric regulations with broad exceptions, and technically allows e-governance penetration to expand state capacity without corresponding checks.

The cases' comparative outcome demonstrates that the political regime is the enabling (or disabling) condition for other variables. Due to that, it is possible to say that the introduction of AI-enabled e-governance occurs within fundamentally different risk architectures: in Estonia, it is absorbed into a system of pre-existing constraints; in Kazakhstan, it introduces a new tool into a system with few constraints, thereby heightening the risks to privacy and data protection. Still, the right to access data benefits in both systems.

4.1.5. Political Will and Strategic Priorities

In the context of other variables, political will and priorities are the most changeable factors, which can potentially override the influence of the other variables[13]. However, the analysis of this variable with respect to Kazakhstan and Estonia reflected the underlying political regime and legal structure. The findings demonstrate a clear alignment between regime-derived priorities and the resulting rights environment.

In Estonia, political will is oriented towards human-centric governance and the reinforcement of democratic values, reflecting a post-conventional level of moral reasoning where state action is justified by universal principles. The national AI strategy and associated investments are framed around building a "citizen-oriented AI

[13] The relationship between political regime type and political will is beyond the scope of this research. However, I believe it is important to briefly discuss it in this section, as it is clearly evident in the cases analysed. The existing literature suggests that political will and priorities can be variable (Beisheim et al., 2025), but the cases examined in this research do not support that notion.

ecosystem" and a "digital state based on transparency, accountability, and human-centric governance." This narrative connects technological advancement with strengthening societal trust and upholding human rights. The political commitment thus acts as a positive, generative force, channelling resources and policy focus towards embedding rights safeguards into the architecture of AI-enabled e-governance.

In Kazakhstan, the political focus is on improving administrative efficiency, modernising the economy, and maintaining state control, while still adhering to a conventional level of moral reasoning. The national discourse, as reflected in initiatives like the "Digital Kazakhstan" program and the AI Concept (2024-2029), portrays AI integration as a method for automating bureaucratic processes, creating a "unified registry of state functions," and eliminating redundancy. This perspective influences a regulatory approach that prioritises facilitating data flow and algorithmic processing for the state. However, it is important to note that the right to access information is promoted in the context of AI-enabled e-governance in Kazakhstan, primarily through third parties.

The comparative outcome reveals that strategic priorities serve as a litmus test for the state's goals. Therefore, the variable of political will and strategic priorities does not operate independently, but, in the analysed cases, it is rather a reflection of the political regime, and it channels the development of e-governance systems towards either empowerment or control, directly impacting the lived experience of privacy, data protection, and access to information.

4.2. Explaining Divergence

The comparison of Estonia and Kazakhstan across five independent variables demonstrates how AI-enabled e-governance affects the realisation of human rights (See Appendix B). A key finding is that this impact depends on factors related to the state, with the type of political regime acting as a meta-variable that shapes the characteristics and interactions of other factors. As a result, the regime type influences whether the transformative potential of AI is directed towards citizen empowerment or towards state control.

Additionally, the analysis reveals that state-related factors significantly affect the realisation of rights related to privacy, data protection, and access to information,

particularly in the health sector. Based on this, I argue that in an e-governance system, AI does not operate independently; instead, it amplifies existing governance structures. The differences between Estonia and Kazakhstan stem not primarily from technological disparities, but from the fundamentally different governance philosophies that underlie their digital states.

4.3. Answering the Research Questions

This thesis is guided by two main research questions aimed at exploring the relationship between AI-enabled e-governance and the realisation of specific fundamental human rights within a comparative context. This section provides answers to these research questions.

Answer to the Research Question 1. There are significant regulatory differences between Kazakhstan and Estonia at all levels. However, these differences are not primarily about the existence of laws or the ratification of international human rights agreements. Instead, they are rooted in the binding power of these laws, their internal coherence, and their normative objectives.

At the international Level, both states are parties to the core UN human rights treaties, including the ICCPR and the ICESCR. The critical difference, however, is in the domestic legal force and implementation of these commitments.

At the Regional Level, the difference is the biggest and structurally consequential. Estonia is embedded within the supranational legal order of the European Union. This subjects the state to the directly applicable regulations and human rights protection institutions, which provide enforcement mechanisms. Kazakhstan, by contrast, participates in regional organisations that produce only non-binding recommendations, model laws, and strategic concepts. This results in an absence of compulsory regional oversight or directly enforceable legal standards for any of the three human rights analysed.

At the national level, Estonia constructed a citizen-centric legal architecture. Its Constitution separately guarantees all three rights, and laws transpose EU norms, creating a unified regime. Kazakhstan's national framework, while formally extensive, is fragmented and state-centric. The 2025 AI Law did not introduce new safeguards, reinforcing the inconsistency of legislation.

In summary, Estonia's regulatory environment is multi-layered, binding, and empowering, actively constraining state action to protect all three rights. Kazakhstan's environment is symbolic at the international level, non-binding at the regional level, and permissive at the domestic level, facilitating state control and making the realisation of privacy, data protection, and access to information highly contingent on political priorities rather than firm legal guarantees.

Answer to the Research Question 2. The extent of AI's impact is reasonably different in each case, and it is determined by the political regime and its resultant variables. However, the impact on the analysed human rights is not equal, as the analysis revealed rights to privacy and data protection to be more vulnerable to the impact of AI-enabled e-governance, while the impact on the right to access information is likely to be positively affected in the health sector.

In Estonia, the introduction of AI has a controlled, neutral to positive effect on the realisation of the analysed human rights. For access to information, AI integration enhances the efficiency and accessibility of personal health data through state-guaranteed platforms. For privacy and data protection, the impact is held within a framework of accountability, where violations occur but are followed by institutional response. In other words, the system demonstrates an institutional capacity to identify and mitigate new risks through legal adaptation.

In Kazakhstan, the introduction of AI in e-governance systems negatively impacts the realisation of the rights to privacy and data protection, while having a neutral to positive effect on information accessibility. The existing regulation of AI-enabled e-governance amplifies vulnerabilities. The risks to privacy and data protection are increased by broad legal exceptions and the absence of technical controls for citizens. Regarding access to information, AI facilitate access through commercial third-party platforms. However, this access is not a state-guaranteed right enshrined in law, and it carries risks of exclusion and lack of accountability.

Consequently, the answer can be formulated as follows: the extent of AI-enabled e-governance impact is a function of the pre-existing governance infrastructure (See Appendix C). However, human rights have different levels of vulnerability toward the

introduction of AI-enabled e-governance, where those ensuring more control for the government are more vulnerable.

4.4. Theoretical and Policy Implications

I believe that the findings of this study are helpful and interesting for both academic discussions and the practical design of AI-enabled e-governance in the era of rapid technological development.

4.4.1. Theoretical Implications

This research reveals the explanatory power of Kohlberg's Theory of Moral Development to the analysis of political regime type and political will and priorities with respect to the emerging topic of AI-enabled e-governance. The comparative findings indicate that these state-related factors correspond to distinct stages of moral reasoning about the relationship between the state and the individual, when it comes to the emerging technological advancements, such as AI-enabled e-governance.

Estonia's consolidated liberal democracy generates a form of political will oriented toward human-centric governance and the reinforcement of democratic values. This aligns with Kohlberg's post-conventional stage of moral reasoning. At this stage, governance is justified by universal ethical principles. This explains why Estonia's digital strategy frames AI as a tool for a "citizen-oriented ecosystem" and why its legal architecture empowers the individual with control mechanisms against potential state overreach. Contrarily, Kazakhstan's consolidated authoritarian regime fosters a political will focused on administrative efficiency, state control, and system maintenance. The primary moral driver is maintaining the social order and respecting authority.

The findings support the theory, showing that at higher stages of reasoning (from the 4th), individuals perceive society as a whole and recognise that norms can be changed through democratic means (Crain 2024, 118-13). My analysis with the help of the theory also illustrates that the current stage of moral reasoning can provide insights into the impact of emerging technologies, such as AI-enabled e-governance, on the realisation of human rights.

In the context, Kohlberg's theory moves beyond describing institutional differences to explaining the normative foundation that makes those differences coherent and self-

reinforcing within each system. It clarifies why “political will” is not an independent variable but is rooted in the moral logic of the political regime itself (Simply Psychology 2023). Consequently, the cases illustrate that human rights are overseen with respect to the political regime, and political will in the discussed cases is an indicator, although theoretically it could be a driving variable.

The study highlights that the impact of AI-enabled e-governance on human rights realisation varies depending on the specific human right in question. It illustrates that Elena Karahanna's Information Boundary Theory, which posits that individuals are inclined to set boundaries, does not fully align with the findings of this analysis. In authoritarian regimes, individuals lack the technical tools to set such boundaries. In contrast, in democratic settings, they are provided with opt-out mechanisms, reducing the need for proactivity on their part. Ultimately, in the era of digital connectivity, individuals' ability to set boundaries is increasingly influenced by the technological frameworks around them rather than their personal intentions, making access to information more accessible as a human right.

4.4.2. Policy Implications

The comparative analysis of Estonia and Kazakhstan provides a set of policy recommendations across different levels of governance. These implications stem from a core finding: the impact of AI-enabled e-governance on human rights is not technologically predetermined but is shaped by the political and institutional environment.

For International Organisations, the study highlights the limitations of promoting model laws without adaptation to existing national laws and support for the institutions that give them force. In contexts for Kazakhstan, where binding regional frameworks are absent, technical assistance should focus on building procedural capacity. This means prioritising the development of operational tools such as standardised methodologies for data protection impact assessments, protocols for algorithmic auditing, and secure digital identity management systems that can function within existing administrative structures. Finally, supporting the creation of inclusive, multi-stakeholder dialogue platforms is crucial.

For national policymakers, actions needed may vary depending on the political context. In consolidated democracies like Estonia, the main challenge is to reinforce and adapt proactively to ongoing issues. Continued investment in the expertise and independent oversight bodies maintains a positive trajectory.

In contrast, for authoritarian or hybrid regimes like Kazakhstan, the primary focus should be on building primary safeguards and reducing systemic risks. This requires a gradual strategy rather than isolated legal reforms. Important initial steps include establishing laws that mandate explicit and informed consent for processing sensitive health data, as well as creating a state-guaranteed mechanism that allows individuals to access their personal data and control who can access it, separate from third parties.

For All States and Technology Developers, the study shows a universal principle: digital infrastructure and tools amplify existing governance logic. Therefore, the architecture of e-governance systems must be consciously engineered to embody higher standards of accountability. Finally, the most significant conclusion is that the pursuit of ethical AI in public administration is inseparable from the quality of governance itself. The most sophisticated digital platform will reflect the values of the system that controls it. Thus, the most effective long-term strategy for protecting human rights in an AI-enabled future is the strengthening of transparent, accountable, and participatory political institutions.

CHAPTER 5. CONCLUSION

This thesis analyses the impact of AI-enabled e-governance on the realisation of human rights, with a specific focus on the rights to privacy, data protection, and access to information within the health sectors of Estonia and Kazakhstan from 2015 to 2025. Through a comparative analysis guided by the MSSD, the study aimed to test the hypothesis that AI-enabled e-governance influences the realisation of human rights.

The findings confirm the central hypothesis. AI-enabled e-governance impacts the realisation of human rights, but it does not autonomously determine outcomes. Instead, it acts as a catalytic amplifier of the pre-existing governance environment. The comparative analysis revealed a clear causal hierarchy among the independent variables, where political regime type emerged as the meta-variable. Finally, the level of e-governance penetration served as an amplifier: in Estonia, high digitalisation

empowers citizens within a rights-based framework; in Kazakhstan, it expands the state's oversight and data-processing capacity.

My research contributes to academic discourse by moving beyond normative assessments of AI ethics. It empirically demonstrates that the human rights implications of algorithmic governance are inseparable from the political and institutional ground on which they are developing. The application of Kohlberg's Theory of Moral Development helped explain the normative foundations of each regime's approach, framing Estonia's as post-conventional (principled) and Kazakhstan's as conventional (system-maintaining). Furthermore, the study nuances the understanding of different rights, showing that within AI-enabled systems, the rights to privacy and data protection are more vulnerable to erosion, while the right to access information often receives a technical boost.

5.1. Limitations and Avenues for Future Research

This study has several limitations that can be considered for further research.

Firstly, as of December 2025, AI in e-governance remains an emerging field. The rapid evolution of both technology and legislation means that this analysis provides a snapshot in time, and its findings may be devalued by new developments. The lack of legal jurisprudence on AI-specific human rights violations in the studied period is a notable data gap, which may indicate either an absence of violations or a lag in their legal recognition and recording.

Secondly, the case selection, while justified by the MSSD methodology, limits the generalizability of the conclusions. The findings are most relevant to countries sharing similar digital ambitions and post-Soviet contexts but differing in political regime. Future research would benefit from expanding the comparative lens to include countries with lower levels of e-governance penetration or from different regional and developmental contexts.

Methodologically, this research relied on legal and policy analysis of primary and secondary sources. Thus, the analysis could be enriched by mixed-methods approaches. Quantitative surveys of citizens and qualitative interviews with policymakers, developers, and civil society representatives would provide important ground-level insights that complement my top-down institutional analysis.

Finally, as a researcher, I acknowledge an inherent asymmetry in expertise. While my effort was to use official sources, the analysis of Estonia was conducted primarily through materials in official translation to English, whereas Kazakh sources were accessed in their original language. This, combined with the inherent constraints of open-source research, means that some details could be overlooked.

5.2. Final Reflections

In conclusion, in this thesis, I argue that the journey toward ethical and rights-respecting AI-enabled governance is not a technical challenge but a governance one. The ultimate impact of the digital transformation of governance on human dignity depends on the political values and institutional structures. Technology will mirror the values of the system it serves. Therefore, the most critical investment for a human-centric digital future is not in algorithms alone, but in the democratic foundations that ensure those algorithms remain tools for liberation, not instruments of control.

BIBLIOGRAPHY

Abdrassulova, A. E., and Yu.S. Kostyanaya. 2025. "Protection of Medical Data in the Provision of Consumer Services: A Comparative Analysis of Some Aspects of Medical Ethics in Kazakhstan and the European Union." *Bulletin of the Karaganda University. "Law Series"* 30 (3(119)): 37–43. doi:10.31489/2025l3/37-43.

Abri, Dhiyab Al, Tanya McGill, and Michael Dixon. 2009. "Examining the Impact of E-Privacy Risk Concerns on Citizens' Intentions to Use e-Government Services: An Oman Perspective." *Journal of Information Privacy and Security* 5 (2): 3–26. doi:10.1080/15536548.2009.10855861.

Anckar, Carsten. 2008. "On the Applicability of the Most Similar Systems Design and the Most Different Systems Design in Comparative Research." *International Journal of Social Research Methodology* 11 (5): 389–401. doi:10.1080/13645570701401552.

Akhmetova, Saule. 2023. "Principles Of Protection Of Personal Data: Comparative Analysis Of Kazakhstan And Foreign Legislation." *Mondaq*, June 21, 2023. Accessed December 1, 2025. https://www.mondaq.com/privacy-protection/1332636/principles-of-protection-of-personal-data-comparative-analysis-of-kazakhstan-and-foreign-legislation.

Akman, Ibrahim, Ali Yazici, Alok Mishra, and Ali Arifoglu. 2005. "E-Government: A Global View and an Empirical Evaluation of Some Attributes of Citizens." *Government Information Quarterly* 22 (2): 239–57. doi:10.1016/j.giq.2004.12.001.

Al-Ansi, Abdullah M., Askar Garad, Mohammed Jaboob, and Ahmed Al-Ansi. 2024. "Elevating E-Government: Unleashing the Power of AI and IOT for Enhanced Public Services." *Heliyon* 10 (23): 1–14. doi:10.1016/j.heliyon.2024.e40591.

Al-Besher, Abdulaziz, and Kailash Kumar. 2022. "Use of Artificial Intelligence to Enhance E-Government Services." *Measurement: Sensors* 24 (December): 1–5. doi:10.1016/j.measen.2022.100484.

Ali, Muhammad. 2023. "E-Governance and E-Democracy: A Digital Revolution." *SSRN Electronic Journal*, November, 1–134. doi:10.2139/ssrn.4623414.

Androutsopoulou, Aggeliki, Nikos Karacapilidis, Euripidis Loukis, and Yannis Charalabidis. 2019. "Transforming the Communication between Citizens and

Government through AI-Guided Chatbots." *Government Information Quarterly* 36 (2): 358–67. doi:10.1016/j.giq.2018.10.001.

Backus, Michiel. 2001. "What Is E-Governance?" Essay. In *Bibliotheca Alexandrina*, 1–47. The Hague, The Netherlands: IICD. https://bibalex.org/baifa/en/resources/document/288383.

Banisar, David. 2011. *Right to Information and Privacy: Balancing Rights and Managing Conflicts*. Washington DC, USA: The International Bank for Reconstruction and Development / The World Bank.

Bannister, Frank, and Regina Connolly. 2012. "Defining E-Governance." *E-Service Journal* 8 (2): 3–25. doi:10.2979/eservicej.8.2.3.

Beisheim, Marianne, Muriel Asseburg, Eric J. Ballbach, Karoline Eickhoff, Sabine Fischer, Nadine Godehardt, Gerrit Kurtz, et al. 2025. "Politics Matters! Political Will as a Critical Condition for Implementing the Sustainable Development Goals." *Earth System Governance* 24 (April): 100244. doi:10.1016/j.esg.2025.100244.

Björklund, Fredrika. 2016. "E-Government and Moral Citizenship: The Case of Estonia." *Citizenship Studies* 20 (6–7): 914–24. doi:10.1080/13621025.2016.1213222.

Brinkerhoff, Derick W. 2010. "Unpacking the Concept of Political Will to Confront Corruption." *Bergen: Chr. Michelsen Institute* , U4 Brief 2010:1, , 1–4.

Cancela-Outeda, Celso. 2024. "The EU's AI Act: A Framework for Collaborative Governance." *Internet of Things* 27 (October): 1–11. doi:10.1016/j.iot.2024.101291.

Civil society report submitted to the United Nations Human Rights Committee. 2025a. *Civil Society Submission on Kazakhstan under the ICCPR (INT/CCPR/CSS/KAZ/63373)*. UN Treaty Body Database, Office of the High Commissioner for Human Rights. Submitted May 26, 2025. Accessed November 19, 2025. https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=INT/CCPR/CSS/KAZ/63373.

Civil society report submitted to the United Nations Human Rights Committee. 2025b. *Civil Society Submission on Human Rights in Kazakhstan under the International Covenant on Civil and Political Rights (INT/CCPR/CSS/KAZ/63263)*. UN Treaty Body Database, Office of the High

Commissioner for Human Rights. Submitted May 26, 2025. Accessed November 19, 2025. https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=INT/CCPR/CSS/KAZ/63263andLang=en.

Commentary on Article 18 of the Constitution of the Republic of Kazakhstan (Комментарий к статье 18 Конституции Республики Казахстан). 2025. In *Constitution of the Republic of Kazakhstan with Commentary*. Accessed January 4, 2026. https://constitutionrk.kz/razdel-2/statya-18.

Conduah, Andrew Kweku, Sebastian Ofoe, and Dorothy Siaw-Marfo. 2025. "Data Privacy in Healthcare: Global Challenges and Solutions." *DIGITAL HEALTH* 11 (May): 1–19. doi:10.1177/20552076251343959.

Conference of the Representatives of the Governments of the Member States. 2012. *Consolidated Version of the Treaty on the Functioning of the European Union, OJ L. 326/47-326/390*, 26 October 2012. European Union. Accessed January 3, 2026. https://www.refworld.org/legal/agreements/eu/2012/en/122600.

Cooley, Charles H. 1907. "Social Consciousness." *American Journal of Sociology* 12 (5): 675–94. doi:10.1086/211543.

Costa Val Rodrigues, Gabriel. 2023. "Human Rights, Interpretivism, and the Semantic Sting." *Canadian Journal of Law andamp; Jurisprudence* 37 (1): 1–29. doi:10.1017/cjlj.2023.10.

Council of Europe, Consultative Committee of Convention 108. 2018. *Opinion on the Request for Accession by the Republic of Kazakhstan (T-PD(2018)19)*, Strasbourg, 12 October 2018. Accessed January 4, 2026. https://rm.coe.int/opinion-on-the-request-for-accession-by-the-republic-of-kazakhstan/16808e56fa.

Council of Europe. 1950. *European Convention on Human Rights, as amended by Protocols Nos. 11, 14 and 15 (ETS No. 005)*. November 4, 1950. https://www.refworld.org/legal/agreements/coe/1950/en/18688.

Council of Europe. 1981. *Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data, ETS 108*, 28 January 1981. Accessed December 30, 2025. https://www.refworld.org/legal/agreements/coe/1981/en/31908.

Court of Justice of the European Union (CJEU). 2021. *Judgment of the Court (Grand Chamber) of 2 March 2021, Case C-746/18, H. K. v. Prokuratuur.* Accessed

December 20, 2025. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=ecli:ECLI%3AEU%3AC%3A2021%3A152.

Crain, William C. 2024. *Theories of Development: Concepts and Applications*. New York: Routledge, Taylor and Francis Group.

Damumed. n.d. *Damumed: Digital Healthcare Ecosystem for Kazakhstan* (ДамюМед: цифровая экосистема здравоохранения). Accessed January 1, 2026. https://www.damumed.kz/.

Dash, Satyabrata, and Subhendu Kumar Pani. 2016. "E-Governance Paradigm Using Cloud Infrastructure: Benefits and Challenges." *Procedia Computer Science* 85: 843–55. doi:10.1016/j.procs.2016.05.274.

"Data Protection and Privacy." 2025. *National Action Plans on Business and Human Rights*. Accessed December 31. https://globalnaps.org/issue/data-protection-and-privacy/.

"Data Protection." 2025. *European Data Protection Supervisor (EDPS)*. December 22. https://www.edps.europa.eu/data-protection/data-protection_en.

Dawes, Sharon S. 2008. "The Evolution and Continuing Challenges of E-governance." *Public Administration Review* 68 (s1): S86. doi:10.1111/j.1540-6210.2008.00981.x.

Diya, Sabhanaz Rashid. "Applying International Human Rights Principles for AI Governance." *Centre for International Governance Innovation*, 2025. http://www.jstor.org/stable/resrep67633.

e-Estonia. 2024. "AI, E-Governance, and Digital Transformation." *e-Estonia.* Accessed January 4, 2026. https://e-estonia.com/ai-e-governance-and-digital-transformation/.

"E-Government." 2025. *UN E-Government Knowledgebase*. United Nations. Accessed December 30. https://publicadministration.un.org/egovkb/en-us/Overview.

ECCIS. 2024. "In 2025 CIS to Complete Development of Model Law on AI Technologies" (В СНГ в 2025 году завершат разработку модельного закона о технологиях искусственного интеллекта). *ECCIS News*. Accessed January 1, 2026. https://eccis.org/news/28046/v_sng_v_2025_godu_zavershat_razrabotku_modelnogo_zakona_o_tehnologijah_iskusstvennogo_intellekta.

El.kz. 2025. “Personal Medical Booklets Now Available Online on the HR Enbek Portal” (Личные медицинские книжки теперь доступны онлайн на портале HR Enbek). *El.kz*, February 11, 2025. Accessed November 27, 2025. https://el.kz/ru/lichnye-meditsinskie-knizhki-teper-dostupny-onlayn-na-portale-hr-enbek_400012849/.

Engelke, Peter. 2020. “AI, Society, and Governance: An Introduction.” Introduction. In *JSTOR*, 2–25. Atlantic Council. https://www.jstor.org/stable/resrep29327.

ERR News. 2023. “10,000 People’s Data Stolen in Genetic Testing Company Asper Biogene Leak.” *ERR News*, December 14, 2023. Accessed January 4, 2026. https://news.err.ee/1609194952/10-000-people-s-data-stolen-in-genetic-testing-company-asper-biogene-leak.

ERR News. 2024. “Company Fined €3 Million over Apotheka Loyalty Program Data Breach.” ERR News, April 24, 2024. Accessed January 4, 2026. https://news.err.ee/1609791258/company-fined-3-million-over-apotheka-loyalty-program-data-breach.

Err, Err. 2024. “Estonia to Invest €85m in Boosting AI Uptake across Public, Private Sectors.” *ERR*. February 12. https://news.err.ee/1609250613/estonia-to-invest-85m-in-boosting-ai-uptake-across-public-private-sectors.

Espinosa, Victor I., and Antonia Pino. 2024. “E-Government as a Development Strategy: The Case of Estonia.” *International Journal of Public Administration* 48 (2): 86–99. doi:10.1080/01900692.2024.2316128.

Estonia. *Estonia’s 4th Periodic Report under the ICESCR*. Accessed December 3, 2025. https://tbinternet.ohchr.org/_layouts/15/TreatyBodyExternal/DownloadDraft.aspx?key=OcaLSysSNsTFBtgqagSh0Nx21Eqbm+qEPx3FGRSeQPnw2tynxdUbUEhGTfyHqdnh.

Estonia. 2018. *Fourth Periodic Report Submitted to the Human Rights Committee under Article 40 of the International Covenant on Civil and Political Rights, Due in 2017.* UN Doc. CCPR/C/EST/4. https://digitallibrary.un.org/record/1639831?ln=frandv=pdf.

“Estonia: Supreme Court Refers AML and Data Protection Case to CJEU for Preliminary Ruling.” 2025. *Dataguidance*. March 25. https://www.dataguidance.com/news/estonia-supreme-court-refers-aml-and-data-protection.

Estonian Human Rights Centre. 2017. “Here’s How Privacy Is Violated in Estonia.” *Liberties.eu,* December 29, 2017. Accessed January 4, 2026. https://www.liberties.eu/en/stories/privacy-violated-estonia/13795.

Eurasian Economic Commission (EEC). 2020. *Strategic Directions for Developing Eurasian Economic Integration until 2025 Approved by Heads of the Eurasian Economic Union States.* News release, December 11, 2020. Accessed November 22, 2025. https://eec.eaeunion.org/en/news/11-12-2020-02/.

European Court of Human Rights. 2019. *Liblik and Others v. Estonia, Application Nos. 173/15, 181/15, 374/15, 383/15, 386/15, 388/15, Judgment of 28 May 2019*. HUDOC. Accessed December 3, 2025. https://hudoc.echr.coe.int/eng?i=001-193251.

European Union, *Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients’ rights in cross-border healthcare*. Accessed January 3, 2026, https://eur-lex.europa.eu/eli/dir/2011/24/oj/eng.

European Union. 2007. *Charter of Fundamental Rights of the European Union, 2012/C 326/02*, 14 December 2007. https://www.refworld.org/legal/agreements/eu/2007/en/13901.

European Union. 2016. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).* Accessed January 3, 2026. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504.

European Union. *Charter of Fundamental Rights of the European Union. 2012/C 326/02.* December 14, 2007. https://www.refworld.org/legal/agreements/eu/2007/en/13901.

e-Estonia. 2021. “Estonia – a European and Global Leader in the Digitalisation of Public Services.” *e-Estonia*, November 15, 2021. Accessed January 3, 2026. https://e-estonia.com/estonia-a-european-and-global-leader-in-the-digitalisation-of-public-services/.

e-Estonia. 2025. *e-Estonia Guide: The Most Advanced Digital Society That Saves Time and Money, updated 08 April 2025*, PDF. Accessed January 3, 2026.

https://www.e-estonia.com/wp-content/uploads/eestonia_guide_08-04-2025.pdf.

FedScoop. 2025. “Ambassador Kristjan Prikk on How Estonia Is Embracing AI for Proactive Citizen Services.” *FedScoop*. Accessed January 4, 2026. https://fedscoop.com/video/ambassador-kristjan-prikk-on-how-estonia-is-embracing-ai-for-proactive-citizen-services/.

Freedom House. 2024. *Estonia: Freedom in the World 2024 Country Report.* Freedom House. Accessed January 3, 2026. https://freedomhouse.org/country/estonia/freedom-world/2024.

Freedom House. 2025. *Kazakhstan: Country Profile*. Freedom House. Accessed January 1, 2026. https://freedomhouse.org/country/kazakhstan.

Fried, Charles. 1968. “Privacy.” *The Yale Law Journal* 77 (3): 475–93. doi:10.2307/794941.

Govering AI for Humanity Final Report High-Level Advisory Body on Artificial Intelligence. 2024. New York, NY: United Nations.

Grigalashvili, Vepkhvia. 2022. “E-Government and E-Governance: Various or Multifarious Concepts.” *International Journal of Scientific and Management Research* 05 (01): 183–96. doi:10.37502/ijsmr.2022.5111.

Grigoryan, Astghik. 2019. “Estonia: Government Issues Artificial Intelligence Report.” *The Library of Congress*. https://www.loc.gov/item/global-legal-monitor/2019-07-31/estonia-government-issues-artificial-intelligence-report/.

Haataja, Samuli. 2018. “The 2007 Cyber Attacks against Estonia.” *Cyber Attacks and International Law on the Use of Force*, December, 111–35. doi:10.4324/9781351057028-5.

Haidar, Aliya. 2025. “Digital Kazakhstan: Pioneering E-Government and AI Innovations Amid New Challenges.” *The Times of Central Asia*, January 1, 2025. Accessed January 4, 2026. https://timesca.com/digital-kazakhstan-pioneering-e-government-innovation-amid-new-challenges/.

Haughton, Odayne, and David Barnes. 2023. “A Comparative Analysis of E-Government in Jamaica and Singapore: An Exploratory Study of Supply-Side Factors.” *Journal of Global Information Technology Management* 26 (2): 116–44. doi:10.1080/1097198x.2023.2200395.

Inform-Kazakhstan. 2025. “Digitalisation of Healthcare: Kazakhstan Will Create a Unified Ecosystem by 2026” (Цифровизация медицины: Казахстан создаст

единую экосистему к 2026 году). *Inform.kz*, January 25, 2025. Accessed January 4, 2026. https://www.inform.kz/ru/tsifrovizatsiya-meditsini-kazahstan-sozdast-edinuyu-ekosistemu-k2026-godu-4c22e7.

Infotrükk Ltd. 1998. *Principles of Estonian Information Policy*. https://ega.ee/wp-content/uploads/2020/01/Eesti-infopoliitika-p-hialused.pdf.

Invest Estonia. 2024. "Estonia Ranks High in the UN E-Government Survey." *Invest in Estonia.* Accessed January 3, 2026. https://investinestonia.com/estonia-ranks-high-in-the-un-e-government-survey/.

Ius Laboris. 2024. "Kazakhstan: The Impact of the GDPR Outside the EU." *Ius Laboris Insights,* March 20, 2024. Accessed January 4, 2026. https://iuslaboris.com/insights/kazakhstan-the-impact-of-the-gdpr-outside-the-eu/.

Jan, Muhammad Ayub. 2025. "Democratic Disconnect in E-Government Policy Initiatives of Khyber Pakhtunkhwa." *FWU Journal of Social Sciences* 19 (March): 113–20. doi:10.51709/19951272/spring2025/10.

Janssen, Marijn, and Natalie Helbig. 2018. "Innovating and Changing the Policy-Cycle: Policy-Makers Be Prepared!" *Government Information Quarterly* 35 (4): 1–7. doi:10.1016/j.giq.2015.11.009.

Karamagioli, Evika. 2008. "From eGovernment to Elnclusion." *The Journal of International Communication* 14 (2): 87–101. doi:10.1080/13216597.2008.9674734.

Khalid, A. 2016. "The E-Governance (E-GOV) Information Management Models." *International Journal of Applied Information Systems* 11 (1): 10–14. doi:10.5120/ijais2016451567.

Kohlberg, Lawrence. 1973. "The Claim to Moral Adequacy of a Highest Stage of Moral Judgment." *The Journal of Philosophy* 70 (18): 630–45. doi:10.2307/2025030.

Koops, Bert-Jaap, Bryce Clayton Newell, Tjerk Timan, Ivan Škorvánek, Tom Chokrevski, and Maša Galič. "A Typology of Privacy." University of Pennsylvania Journal of International Law 38, no. 2 (2017): 487–494. *Tilburg Law School Research Paper No. 09/2016*. https://ssrn.com/abstract=2754043.

Kratid. n.d. AI Mapping and Algorithms in Use in the Public Sector. *Kratid*. Accessed November 24, 2025. https://www.kratid.ee/en/algoritm-ulevaade.

KT.kz. 2024. “Artificial Intelligence Should Be Used Ethically and Responsibly” (Искусственный интеллект должен использоваться этично и ответственно). *KT.kz*, November 15, 2024. Accessed January 6, 2026. https://www.kt.kz/rus/science/iskusstvennyy_intellekt_dolzhen_ispolzovatsya_1377982704.html.

Kursiv Media. 2024. “Two Ministries and the Prosecutor’s Office of Almaty Are Looking for Those Responsible for the Leak of Personal Data of KazNU Female Students” (Виновных в утечке личных данных студенток КазНУ ищут два министерства и прокуратура Алматы). *Kursiv.kz,* February 14, 2024. Accessed November 27, 2025. https://kz.kursiv.media/2024-02-14/tksh-utechka-dannyye-kaznu/.

Kursiv Media. 2025. “Almaty Police Investigate Possible Leak of HIV Patient Data” (В Алматы проверяют факт утечки данных людей с ВИЧ). *Kursiv.kz*, April 4, 2025. Accessed November 27, 2025. https://kz.kursiv.media/2025-04-04/smrd-almaty-sliv-vich/.

Lever, Annabelle. 2006. “Privacy Rights and Democracy: A Contradiction in Terms?” *Contemporary Political Theory* 5 (2): 142–62. doi:10.1057/palgrave.cpt.9300187.

Linis-Dinco, Jean. 2024. *FoundationBalancing Progress and Human Rights: Is Thailand Ready for Artificial Intelligencethat Respects Human Rights? Trust.Org*. Manushya Foundation. https://www.trust.org/wp-content/uploads/2024/12/AI-Study-Report_Rev4_2024_11_05.pdf.

Margetts, Helen, and Andre Naumann. "Government as a platform: What can Estonia show the world." Research paper, University of Oxford 1, no. 1 (2017): 1-41.

Margetts, Helen. 2022. “Rethinking AI for Good Governance.” *Daedalus* 151 (2): 360–71. doi:10.1162/daed_a_01922.

Ministry of Artificial Intelligence and Digital Development of the Republic of Kazakhstan (MAIDD). 2025. “2025 Results: Kazakhstani Citizens Increasingly Receive Public Services via Smartphone” (Итоги 2025 г.: казахстанцы все чаще получают госуслуги через смартфон). Government of the Republic of Kazakhstan. Accessed January 4, 2026. https://www.gov.kz/memleket/entities/maidd/press/news/details/1134705?lang=ru.

Ministry of Healthcare of the Republic of Kazakhstan. 2020. *Digital Journey: Kazakhstan's Healthcare.* GOV.KZ, February 18, 2020. Accessed January 4, 2026. https://www.gov.kz/memleket/entities/dsm/press/article/details/4848?lang=en.

Organisation for Economic Co-operation and Development (OECD). 2018. *Digital Agenda 2020 for Estonia.* OECD Country. https://www.oecd-events.org/smart-data-and-digital-technology-in-education/session/d3520a50-d2fe-ec11-b47a-a04a5e7cf9da/digital-agenda-2020-for-estonia.

Organisation for Economic Co-operation and Development (OECD). 2019. *Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449.* Accessed January 3, 2026. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.

Organisation for Economic Co-operation and Development (OECD). 2022. *Health Data Governance for the Digital Age: Implementing the OECD Recommendation on Health Data Governance*. Paris: OECD Publishing. https://doi.org/10.1787/68b60796-en.

Organization for Security and Co-operation in Europe, OSCE Office for Democratic Institutions and Human Rights (ODIHR). 2025. *Trial Monitoring Report, Kazakhstan (November 2022 – December 2023).* Warsaw: OSCE/ODIHR, May 5, 2025. Accessed January 1, 2026. https://odihr.osce.org/odihr/590375.

Our World in Data. "Human rights index – V-Dem." Accessed December 25, 2025. https://ourworldindata.org/grapher/human-rights-index-vdem.

President of the Republic of Kazakhstan, Kassym-Jomart Tokayev. 2024. "Kazakhstan in the Era of Artificial Intelligence: Current Tasks and Solutions Through Digital Transformation" (Послание Главы государства Касым-Жомарта Токаева народу Казахстана "Казахстан в эпоху искусственного интеллекта: актуальные задачи и их решения через цифровую трансформацию"). *Akorda.kz,* September 1, 2024. Accessed January 6, 2026. https://www.akorda.kz/ru/poslanie-glavy-gosudarstva-kasym-zhomarta-tokaeva-narodu-kazahstana-kazahstan-v-epohu-iskusstvennogo-intellekta-aktualnye-zadachi-i-ih-resheniya-cherez-cifrovuyu-transformaciyu-885145.

Prime Minister of the Republic of Kazakhstan. 2023. "eGov Mobile to Expand the eDensaulyq Medical Data Section" (В «eGov mobile» будет расширен раздел

медицинских данных «eDensaulyq»). *PrimeMinister.kz*, March 24, 2023. Accessed November 27, 2025. https://primeminister.kz/ru/news/v-egov-mobile-budet-rasshiren-razdel-meditsinskikh-dannykh-edensaulyq-23474.

Prime Minister of the Republic of Kazakhstan. 2024. “Implementation of Artificial Intelligence in Government Services for Citizens and Businesses Discussed in Government” (Внедрение искусственного интеллекта в государственные сервисы для граждан и бизнеса обсудили в правительстве). *PrimeMinister.kz,* July 24, 2024. Accessed December 22, 2026. https://primeminister.kz/ru/news/vnedrenie-iskusstvennogo-intellekta-v-gosudarstvennye-servisy-dlya-grazhdan-i-biznesa-obsudili-v-pravitelstve-28677.

Prime Minister of the Republic of Kazakhstan. 2025. “Innovations in Public Services: New Digital Solutions for Business and Citizens.” *PrimeMinister.kz,* March 26, 2025. Accessed January 4, 2026. https://primeminister.kz/en/news/innovations-in-public-services-new-digital-solutions-for-business-and-citizens-29877.

Profit.kz. 2025a. “Inventory of Government Functions Begins in Kazakhstan Ahead of AI Implementation” (В Казахстане началась инвентаризация госфункций перед внедрением ИИ). *Profit.kz,* January 23, 2025. Accessed January 1, 2026. https://profit.kz/news/72048/V-Kazahstane-nachalas-inventarizaciya-gosfunkcij-pered-vnedreniem-II/.

Profit.kz. 2025b. “Kazakhstan Is Introducing AI Agents into the Healthcare System” (Казахстан внедряет ИИ-агентов в систему здравоохранения). *Profit.kz,* January 22, 2025. Accessed January 6, 2026. https://profit.kz/news/72013/Kazahstan-vnedryaet-II-agentov-v-sistemu-zdravoohraneniya/.

Prosci. 2025. “People, Process, Technology (PPT) Framework: Pros and Cons.” *Prosci*. Prosci Inc. October 30. https://www.prosci.com/blog/people-process-technology.

Randma-Liiv, Tiina, Rasa Bortkevičiūtė, Veiko Lember, Visvaldis Valtenbergs, and Vitalis Nakrosis. 2025. “Advancing Citizen Engagement through Digital Tools: A Comparative Study of the Baltic States.” *International Journal of Public Administration*, July, 1–16. doi:10.1080/01900692.2025.2517124.

Republic of Estonia, Ministry of Economic Affairs and Communications (MEAC). 2021. *Estonia's Digital Agenda 2030: Development Agenda for Digital Society*. PDF. Accessed January 3, 2026. https://www.mkm.ee/sites/default/files/documents/2022-04/Digiühiskonna%20arengukava_ENG.pdf.

Republic of Estonia, Ministry of Justice and Digital Affairs. 2025. *Estonian National Digital Decade Strategic Roadmap 2025.* PDF, March 2025. Accessed January 3, 2026. https://www.justdigi.ee/sites/default/files/documents/2025-03/Estonian%20National%20Digital%20Decade%20Strategic%20Roadmap%202025.pdf.

Republic of Estonia. 2015. *Penal Code*. Consolidated text, ELI 522012015002. Accessed January 3, 2026. https://www.riigiteataja.ee/en/eli/522012015002/consolide.

Republic of Estonia. 2018. *Civil Code*. Consolidated text, ELI 508012018001. Accessed January 3, 2026. https://www.riigiteataja.ee/en/eli/508012018001/consolide.

Republic of Estonia. 2019. *Personal Data Protection Act*. Consolidated text, ELI 523012019001. Accessed January 3, 2026. https://www.riigiteataja.ee/en/eli/523012019001/consolide.

Republic of Estonia. 2025. *The Constitution of the Republic of Estonia*. Consolidated text, ELI 523042025001. Accessed January 3, 2026. https://www.riigiteataja.ee/en/eli/523042025001/consolide.

Republic of Kazakhstan. 2004. *On the State Program for the Reforming and Development of Healthcare of the Republic of Kazakhstan for 2005–2010* (О Государственной программе реформирования и развития здравоохранения Республики Казахстан на 2005–2010 годы). Decree of the President No. 1438. Adilet Legal Information System. Accessed January 4, 2026. https://adilet.zan.kz/rus/docs/U040001438_.

Republic of Kazakhstan. 2013. *Law of the Republic of Kazakhstan "On Personal Data and Their Protection"* (Закон Республики Казахстан «О персональных данных и их защите», No. 94-V). Adilet Legal Information System. Accessed January 4, 2026. https://adilet.zan.kz/eng/docs/Z1300000094.

Republic of Kazakhstan. 2015. *Law of the Republic of Kazakhstan "On Access to Information"* (Закон Республики Казахстан «О доступе к информации»,

Law No. 401-V, 16 November 2015). Adilet Legal Information System. Accessed January 4, 2026. https://adilet.zan.kz/eng/docs/Z1500000401.

Republic of Kazakhstan. 2017. *On the Approval of the State Program "Digital Kazakhstan"* (Об утверждении Государственной программы "Цифровой Казахстан", Постановление Правительства Республики Казахстан № 827, 12 December 2017). Adilet Legal Information System. Accessed January 4, 2026. https://adilet.zan.kz/rus/docs/P1700000827.

Republic of Kazakhstan. 2020. *Code of the Republic of Kazakhstan "On Public Health and Healthcare System"* (Кодекс Республики Казахстан «О здоровье народа и системе здравоохранения», Code No. 360-VI, 7 July 2020). Adilet Legal Information System. Accessed January 4, 2026. https://adilet.zan.kz/eng/docs/K2000000360.

Republic of Kazakhstan. 2024. *On the Approval of the Concept for the Development of Artificial Intelligence for 2024–2029* (Об утверждении Концепции развития искусственного интеллекта на 2024–2029 годы, Постановление Правительства Республики Казахстан № 592, 24 July 2024). Adilet Legal Information System. Accessed January 1, 2026. https://adilet.zan.kz/rus/docs/P2400000592.

Republic of Kazakhstan. 2025. *Law of the Republic of Kazakhstan "On Artificial Intelligence"* (Закон Республики Казахстан «Об искусственном интеллекте», Law No. 230-VIII, 17 November 2025). Adilet Legal Information System. Accessed January 4, 2026. https://adilet.zan.kz/rus/docs/Z2500000230.

Republic of Kazakhstan. *Constitution of the Republic of Kazakhstan* (Қазақстан Республикасының Конституциясы; Конституция Казахстана). Approved by referendum 30 August 1995, in force 5 September 1995. Accessed January 4, 2026. https://www.akorda.kz/en/constitution-of-the-republic-of-kazakhstan-50912.

Republican Center for Electronic Healthcare (RCEZ). 2025. List of Medical Information Systems (Перечень медицинских информационных систем). *e-Health*. Accessed January 4, 2026. https://rcez.kz/mis.

"Resolution Adopted by the General Assembly on 19 December 2023 (A/RES/78/213)." 2023. United Nations General Assembly.

SAMENA Telecommunications Council. 2024. *Global Digitalization Index 2024*. September 2024. Accessed December 25, 2025. https://www.samenacouncil.org/gdi.

Simply Psychology. 2023. "Kohlberg's Stages of Moral Development." *Simply Psychology.* Accessed January 6, 2026. https://www.simplypsychology.org/kohlberg.html.

Srinivas, Hari. 2025. "Urban E-Governance: Defining E-Governance." *Gdrc.Org*. Global Development Research Center. Accessed December 30. https://www.gdrc.org/u-gov/egov-01.html.

Stanton, Jeffrey M. 2003. "Information Technology andPrivacy: A Boundary Management Perspective." Essay. In *Idea Group Publishing*, 79–93. Idea Group Publishing. https://www.researchgate.net/publication/255590658_Information_Technology_and_Privacy_A_Boundary_Management_Perspective.

"Story - e-Estonia." 2025. *E-Estonia.Com*. Estonian Business and Innovation Agency. April 7. https://e-estonia.com/story/.

UN Economic and Social Council. 2000. *General Comment No. 14: The Right to the Highest Attainable Standard of Health (Art. 12 of the Covenant). E/C.12/2000/4. UN Committee on Economic, Social and Cultural Rights (CESCR)*, August 11, 2000. https://www.refworld.org/legal/general/cescr/2000/en/36991.

UN Human Rights Committee (HRC). 1988. CCPR General Comment No. 16: Article 17 (Right to Privacy), *The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation.* April 8, 1988. https://www.refworld.org/legal/general/hrc/1988/en/27539.

United Nations Committee on Economic, Social and Cultural Rights. 2019. *Concluding Observations on the Third Periodic Report of Estonia. UN Doc. E/C.12/EST/CO/3.* Geneva: United Nations.

United Nations Department of Economic and Social Affairs (UNDESA), Division for Public Institutions and Digital Government (DPIDG). 2025. *United Nations E-Government Knowledgebase Data Center*. UN E-Government Knowledgebase. Accessed January 41, 2026. https://publicadministration.un.org/egovkb/Data-Center.

United Nations Department of Economic and Social Affairs. *E-Government Knowledgebase Data Center.* Accessed December 31, 2025. https://publicadministration.un.org/egovkb/Data-Center.

United Nations Human Rights Committee (UN HRC). 2025. *Concluding Observations on the Third Periodic Report of Kazakhstan (CCPR/C/KAZ/CO/3).* Geneva: UN, September 3, 2025. Accessed November 21, 2025. https://docs.un.org/en/CCPR/C/KAZ/CO/3.

United Nations Human Rights Committee. *Concluding Observations on the Fourth Periodic Report of Estonia. UN Doc. CCPR/C/EST/CO/R.4*. Geneva: United Nations, March 14, 2019. https://digitallibrary.un.org/record/3797047.

United Nations, General Assembly. 1966a. "International Covenant on Civil and Political Rights." *United Nations Treaty Series 999:* 178. Accessed December 31, 2025. https://www.refworld.org/legal/agreements/unga/1966/en/17703.

United Nations, General Assembly. 1966b. "International Covenant on Economic, Social and Cultural Rights." *United Nations Treaty Series 993:* 8. Accessed December 31, 2025. https://www.refworld.org/legal/agreements/unga/1966/en/33423.

Varieties of Democracy (V-Dem) Institute. n.d. *Country Graphs and Data Visualisations.* Accessed January 3, 2026. https://v-dem.net/data_analysis/CountryGraph/.

Vincent, Brandi. 2025. "Estonia Moves to Develop New Cross-Government, AI-Powered Data Management Asset." *DefenseScoop*, April 25, 2025. Accessed November 30, 2025. https://defensescoop.com/2025/04/25/estonia-ai-powered-data-management-tool-ambassador-kristjan-prikk/.

Xu, Jian, Terence Lee, and Gerard Goggin. 2024. "AI Governance in Asia: Policies, Praxis and Approaches." *Communication Research and Practice* 10 (3): 275–77. doi:10.1080/22041451.2024.2391204.

APPENDIX A

Table 3. Operationalisation of Variables

Variable	Type of measurement	Means of Measurement
I.V.1: State commitments to international and regional HR instruments	Empirical, Normative	Status of ratification of relevant international treaties. Values: ratified / signed / not signed (null). Scope of commitment and implementation based on state reports, concluding observations, and assessments from international and regional monitoring bodies (e.g., UN HRC, Council of Europe, OSCE, CIS structures). Values: strong / moderate / weak (null) – content analysis.
I.V.2: National E - governance regulations	Normative	Assessment of the presence and scope of legal frameworks on e-governance concerning: the analysed rights. Values: comprehensive / partial / absent (null) – content analysis of documents.
I.V.3: E-governance penetration (as ICT infrastructure)	Normative	Scope of digitalisation of public services: fully digitalised / partially digitalised / not digitalised (null) – based on indices.
I.V.4: Political regime type	Normative	Regime category: Working democracy / Deficient democracy / Moderate autocracy / Hard autocracy (null) – based on indices.
I.V.5: Political will & Strategic Priorities	Empirical	Evidence of commitment in official strategies, laws, speeches: Human rights prioritised / not prioritised (null) – content analysis of documents.
D.V.: AI impact on HR realisation in e-governance	Normative	Legal and policy frameworks addressing human rights risks (privacy) in AI use. Values: protective / partially protective / no regulation (null) – content analysis of documents.
	Empirical	Actual outcomes as reflected in case studies, secondary reports: positive / negative / no observable impact (null) – content analysis.

APPENDIX B

Table 4. Systematic Comparison of Findings

Variable	Estonia	Kazakhstan	Comparative Outcome & Impact on Rights Realisation
I.V.1: State Commitments to International & Regional HR Instruments	Binding Regional Framework (EU). Subject to direct application of GDPR, EU Charter, AI Act.	Non-binding Regional Influences. Party to ICCPR/ICESCR but subject only to soft law from OSCE, EAEU, CIS.	Primary Difference: Supranational Enforcement.Estonia's EU membership actively bridges international norms and domestic law. Kazakhstan's lack of binding regional oversight creates a significant gap between ratification and realisation.
I.V.2: National E-governance Regulations	Comprehensive, Citizen-Centric, Adaptive. Health Services Act provides opt-out & access logs. Framework prioritises individual control.	Fragmented, State-Centric, Permissive. Health code uses implicit consent. Laws prioritise administrative efficiency and state data access.	Estonia’s framework establishes individual agency as the default, enabling active exercise of rights. Kazakhstan’s framework establishes state access as the default, rendering rights passive and conditional.
I.V.3: E-governance Penetration	High Penetration with Integrated User Control. Near-total digitisation. Infrastructure includes tools for citizen empowerment: access logs, state-guaranteed information portals (terviseportaal.ee), and opt-out mechanisms.	High Penetration without Effective User Control. Widespread digitisation. Data entry often automatic/implicit. Access to information mediated by commercial third-party platforms via user agreements, not state guarantee.	The Amplifier Effect. In Estonia, high penetration amplifies citizen empowerment, making rights exercise more efficient. In Kazakhstan, it amplifies state/corporate data capacity and control, increasing risks to privacy/data protection and offering a fragile form of information access.

I.V.4 (M.V): Political Regime Type	Consolidated Liberal Democracy. High scores on judicial independence and privacy safeguards.	Consolidated Authoritarian Regime. Low scores on judicial independence and privacy. Power centralised; institutions designed to consolidate control. Rights subordinate to state interests.	The Foundational Meta-Variable. Regime type creates the enabling/disabling environment. Estonia's democracy enforces commitments and generates citizen-centric law. Kazakhstan's authoritarianism insulates government and produces state-centric law.
I.V.5: Political Will & Strategic Priorities	Human-Centric Governance & Democratic Values. AI strategy framed around "citizen-oriented ecosystem," transparency, and accountability.	Administrative Efficiency & State Control. AI agenda focused on automating bureaucracy, creating state function registries, and system integrity.	Priorities express the regime's moral logic. Estonia's will acts as a positive, generative force for rights safeguards. Kazakhstan's will acts as a risk factor, accelerating technological deployment without protective frameworks.
D.V.: Impact on HR Realisation in AI-enabled E-governance	Managed, Neutral to Positive. AI integrated into a system with strong safeguards, oversight, and remedies. Privacy/Data Protection: Uphold within accountability framework. Access to Information: Actively facilitated and enhanced. Systemic capacity to manage new risks.	Negative and Aggravating. AI deployed into a regulatory/institutional vacuum, amplifying vulnerabilities. Privacy/Data Protection:Significantly heightened risks; breaches lack effective remedies. Access to Information: Commercially mediated, not guaranteed. Systematically undermines rights protection.	AI's impact is not inherent but contingent. In Estonia, it is absorbed and constrained by a rights-based system. In Kazakhstan, it amplifies and exacerbates the deficiencies of a state-centric system. The political regime (I.V.4) is the decisive factor shaping this outcome.

APPENDIX C

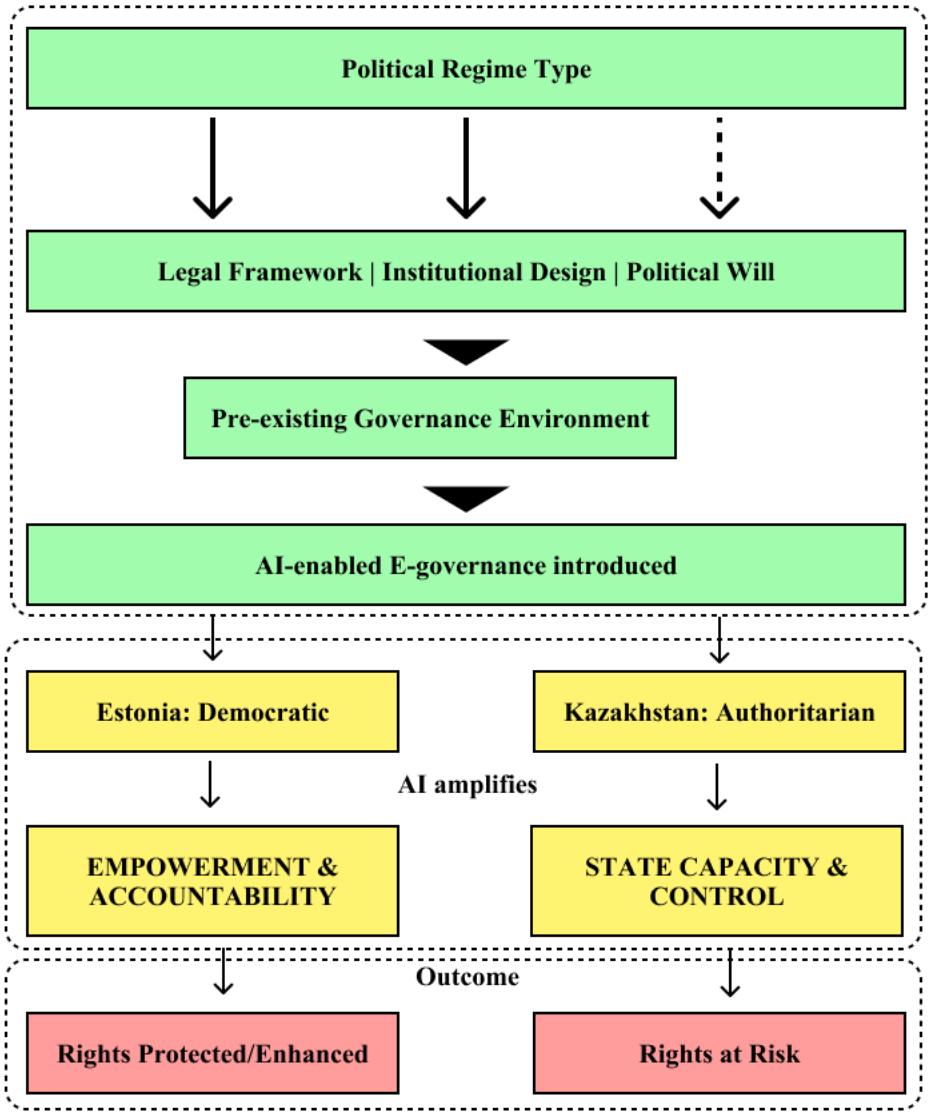

Figure 6. Conceptual Diagram: "The Amplification Model of AI-Enabled E-Governance". Source: created by the author