The Role of Regulatory Frameworks in Shaping E-Governance: Insights from Selected Case Studies

Zoran Jordanoski [a*]

[a] United Nations University - Operating Unit on Policy-Driven Electronic Governance (UNU-EGOV), Guimaraes, Portugal, jordanoski@unu.edu, https://orcid.org/0000-0003-1784-9038.

Submitted: 31 January 2025, Revised: 26 March 2025, Accepted: 21 April 2025, Published: 23 May 2025

Abstract. As digital transformation accelerates globally, the quality of national regulatory frameworks has become a key determinant of effective e-governance. This paper investigates how regulatory maturity influences the development and implementation of digital government initiatives across eight countries. It introduces a three-tier classification: advanced, moderate, and early-stage, based on the scope of legal frameworks, operationalisation of digital enablers, and integration into public service delivery. Countries such as Belgium, Estonia, and Singapore demonstrate that coherent and enforceable legal ecosystems when paired with institutional coordination and technical infrastructure, achieve high digital governance performance. By contrast, fragmented frameworks constrain implementation and trust. Using cross-case comparison and internationally recognised indices (e.g., EGDI, OSI, EPI, GCI), the study validates this classification and identifies recurring barriers such as regulatory lag, institutional misalignment, operational and infrastructure gaps, and societal mistrust. The findings confirm that while legal maturity is foundational, institutional capacity, technical readiness, and public engagement are critical for inclusive and resilient digital transformation.

Keywords. Digital governance, E-Governance, Regulatory Maturity, Legal Framework, Digital Transformation.
Research paper, DOI: https://doi.org/10.59490/dgo.2025.1037

1. Introduction

E-governance has emerged as a cornerstone of modern public administration (Gil-Garcia et al., 2018; Heeks, 2002). It leverages digital technologies to transform the way government operates (Bannister & Connolly, 2011a; Cordella & Bonina, 2012), enhance public service delivery (Meyerhoff Nielsen, 2017; Meyerhoff Nielsen & Krimmer, 2015), increase transparency (Chauhan et al., 2008; López-López et al., 2018) and facilitate citizen engagement (Mahrer & Krimmer, 2005; Navarra & Cornford, 2003). Defined broadly, e-governance refers to the application of Information and Communication Technologies (ICTs) to transform government operations and interactions with citizens, businesses, and other stakeholders (Heeks, 2008; UNDESA, 2022). At its core, e-governance relies on key elements, such as electronic identification (eID) and trust services, interoperability and data exchange systems, electronic payments, and digital communication platforms. Additionally, essential elements include legal frameworks for accessing and reusing public sector information, data protection, and cybersecurity. Together, these frameworks establish the backbone of any transparent, secure, and resilient digital governance ecosystem.

These main elements are underpinned by legal frameworks that regulate their design, implementation, and operation (González et al., 2016; Papadopoulos & Kanellis, 2012; Veit & Huntgeburth, 2014). The quality of regulations is one of the factors determining the practical implementation of these elements and their functionality in practice (Bannister & Connolly, 2011b; Meyerhoff Nielsen & Jordanoski, 2020). Effective regulatory frameworks not only facilitate the implementation of digital solutions but also foster public trust, which is a critical enabler for e-governance adoption (OECD, 2020d). However, adopting a legal framework does not guarantee automatic results or compliance in practice (Jordanoski & Meyerhoff Nielsen, 2023).

Modern legal frameworks play an essential role in e-governance by enabling effective, secure, and transparent service delivery while fostering innovation (Hasan et al., 2015). They also guide governments in adapting to emerging technologies through principles such as technological neutrality and flexibility, which are critical in managing rapid advancements and jurisdictional complexities (Gregory, 2002; Tojiev, 2024). Their adaptability ensures that public sector initiatives remain resilient and capable of meeting evolving societal and technological needs (Korvat, 2023; Park et al., 2016).

The objective of this paper is to examine the relationship between the maturity of regulatory frameworks and the quality of e-governance developments. It provides a high-level analysis of regulatory approaches adopted in Belgium, Botswana, Ecuador, Estonia, Jamaica, Kyrgyzstan, Kenya, and Singapore. It evaluates their practical outcomes, such as the rollout of adequate technical infrastructure, institutional systems, or frameworks. This analysis addresses the following research question: *How do the maturity levels of regulatory frameworks correlate with the development of e-governance in different countries?* While many existing studies focus on theoretical models or isolated national cases, this research offers comparative, empirical insights into how regulatory maturity shapes digital governance across diverse contexts.

The paper is structured as follows: the second section reviews the literature on the research subject. The methodology and how the study was conducted is presented in the third section. The study results and discussion are presented in the fourth section, while the conclusions and future work are included in the last section.

2. Literature Review

The Role of Regulatory Frameworks in E-Governance

Regulation plays a crucial role in shaping the development, implementation, and performance of digital government systems in every country (López-López et al., 2018; OECD, 2020b). The design and implementation of e-governance initiatives are directly influenced by existing legal and policy frameworks (Dovhan et al., 2022; Luna-Reyes et al., 2016). These frameworks provide the necessary legal basis for digital government projects (Luna-Reyes et al., 2016), defining the rules for data handling, service delivery, and citizen engagement. However, the absence of a comprehensive legal framework can lead to uncertainty, increased legal risks, and hinder the adoption of new technologies (Cordella & Bonina, 2012; Muliaro Wafula, 2012).

Effective regulation provides legal clarity, fosters trust, and ensures compliance with privacy and data protection requirements (Chatterjee & N.S., 2022; Hasan et al., 2019). For instance, regulatory frameworks for eID emphasise privacy and security, establishing robust requirements to address potential vulnerabilities in data sharing. Additionally, regulatory frameworks support interoperability and cross-border governance. For example, the experiences of Estonia and Singapore demonstrate how mature regulatory environments encourage both innovation and public adoption of digital government services (Lebid, 2021; Shkarlet et al., 2020). On a cross-border level, the European Health Data Space demonstrates how harmonised regulations can facilitate the secure and efficient exchange of patient health data among public agencies across all EU Member States (Schneider et al., 2024).

International standards and frameworks also significantly influence national regulatory approaches, particularly in areas such as web accessibility (Jordanoski & Meyerhoff Nielsen, 2023), data protection and cybersecurity (Ortega et al., 2023). Adopting these standards can foster interoperability among diverse e-governance systems (Wimmer et al., 2018). However, successful implementation depends not only on adoption but on the ability to adapt such standards to local contexts and administrative capacities. Moreover, the effectiveness of these regulations depends heavily on their enforcement mechanisms and institutional alignment, which vary across jurisdictions.

Despite widespread recognition of regulation's enabling role, the literature remains somewhat fragmented regarding comparative, empirical analyses across diverse country contexts. Most studies focus on either highly developed digital economies or normative frameworks, leaving a gap in understanding how regulation functions in practice across different governance environments.

Technological Advancements and Regulatory Challenges

Technological advancements often outpace regulatory development, creating significant challenges for governments (Dovhan et al., 2022; Luna-Reyes et al., 2016). One prominent challenge is integrating emerging technologies, such as AI and blockchain, within existing legal frameworks without causing fragmentation or inefficiency (Firdaus et al., 2024). Ensuring data privacy with rapid advancements in data analytics and AI remains a pressing issue (Mustafa et al., 2025). While fragmented regulations can undermine public trust and create governance gaps, overly rigid frameworks may hinder innovation. This highlights the need for flexible and adaptive approaches (He, 2011; Nyman-Metcalf, 2014).

The federated approach employed in Europe, which emphasises collaborative governance, serves as a potential model for harmonising regulations across regions with diverse legal and infrastructural landscapes (Krimmer et al., 2021). To remain relevant, regulations should be periodically reviewed and updated through stakeholder collaboration. For example, adaptive regulatory practices have been integral to digital transformation efforts in Estonia and Brazil (Franco, 2024; Okon, 2024). Maintaining a balance between innovation and regulation remains critical to avoiding both regulatory delays and stifling innovation (OECD, 2020b; Ortega et al., 2023). In this context, regulatory maturity should be viewed not only as a function of legal completeness or technical scope but also as a reflection of institutional adaptability and alignment with broader governance models. Legal systems must evolve parallel to complex digital infrastructures, requiring coordinated policy responses and long-term strategic planning.

This review provides the conceptual grounding for the study's core objective: to assess how the maturity of regulatory frameworks correlates with e-governance development across different country contexts. While previous literature has established the foundational importance of regulation, empirical studies examining its operational effectiveness through comparative, multi-country case analysis remain limited. This paper aims to address that gap through a structured, cross-country comparative analysis.

3. Methodology

A classical exploratory, qualitative, comparative case study methodology is applied to address the research gaps related to shaping e-governance through regulatory frameworks (Rohlfing, 2012; Yin, 2017). The approach is needed to understand the complex correlation between regulations and e-governance implementation. By analysing the regulatory practices of eight countries, this study aims to understand how regulations contribute to the development and implementation of e-governance. The research uses a theory-informed, evidence-driven comparative approach to identify patterns across cases while remaining attuned to local contexts (Thornberg, 2012).

Case selection

The study includes eight countries (in alphabetical order: Belgium (BE), Botswana (BW), Ecuador (EC), Estonia (EE), Jamaica (JM), Kenya (KE), Kyrgyzstan (KG), and Singapore (SG)) selected based on a combination of geographic, economic, and cultural diversity and varying degrees of e-governance maturity. The diversity of these cases ensures that the findings reflect a broad spectrum of regulatory capacities and implementation realities rather than being limited to high-income or digitally advanced economies. Case selection also considered the availability of documented legal frameworks, policy materials, and national e-governance initiatives. Table 1 presents the contextual factors, i.e. the key socioeconomic and connectivity indicators for the eight countries to support the comparative analysis that may shape digital governance capacity.

Tab. 1 – Socioeconomic (a-e) (CIA.gov, 2025) and connectivity indicators (f-i) (ITU, 2025).

Indicator	BE	BW	EC	EE	JM	KE	KG	SG
a) Population (millions, 2024 est.)	11.9	2.4	18.3	1,2	2.8	58,2	6.1	6.0
b) Territory (thousands, km^2)	30.5	581.7	283.5	45.2	10.9	580.3	199.9	719.0
c) Urbanisation (%) of total population (2023)	98.2	72.9	64.8	69.8	57.4	29.5	37.8	100
d) GDP (PPP) (billions, USD, 2023 est.)	756.6	46.7	260.2	58.2	29.2	314.5	45.5	754.7
e) GDP per capita (PPP) (thousands, USD, 2023 est.)	64.2	18.8	14.5	42.5	10.3	5.7	6.4	127.5
f) Individuals using the Internet (%)	94	77.3	69.7	91	82.4	40.8	79.8	96
g) Households with Internet access at home (%)	94.4	78.3	60.4	95	75.4	50.2	93.4	98.7
h) Active mobile broadband subscriptions per 100 inhabitants	94.9	108	59.4	210	66.7	59	175	164
i) Population covered by at least a 4G/LTE mobile network (%)	100	91	93.9	99	99	97	96.9	100

The socioeconomic profiles of the eight countries reveal significant disparities. High-income countries such as Singapore and Belgium operate in vastly different resource environments than lower-income peers like Kenya or Kyrgyzstan. These economic conditions directly influence the capacity of the governments to invest in national digital infrastructure and establish robust regulatory oversight bodies, factors repeatedly shown to affect e-governance development. Population size and territorial spread also introduce implementation asymmetries. For instance, Kenya and Botswana have large geographic areas and highly rural populations, making connectivity rollouts and last-mile digital service delivery more logistically and financially demanding. In contrast, Singapore's dense urban environment and compact geography offer inherent efficiencies for digital service scaling.

Finally, while digital infrastructure is not the central focus of this study, it is a key enabling condition that shapes the operational feasibility of e-governance systems. In that regard, several countries demonstrate high levels of internet penetration, household connectivity, and mobile broadband subscriptions, indicating well-established digital infrastructure. These conditions suggest a strong baseline for the delivery and adoption of online government services. In other contexts, infrastructure access remains uneven. Lower household internet access rates, modest broadband subscription levels, and digital divides between urban and rural populations signal potential barriers to inclusive digital service deployment. While mobile network coverage is broadly high, approaching universal 4G availability in most countries, this does not automatically translate into effective usage.

Together, these structural factors help explain why legal reforms alone may not suffice, particularly in low- and middle-income countries. Instead, regulatory ambition must be accompanied by targeted policies that account for economic, geographic, and demographic constraints, ensuring that digital transformation strategies are realistic and inclusive.

Data Sources and Analytical Framework

The primary and secondary sources included official legislative texts, policy documents, official reports, and academic literature. The objective was to identify the common principles, discrepancies, and patterns across the selected jurisdictions. For that purpose, the study employed a cross-case comparative analysis, which enabled the evaluation of the common principles while considering the unique factors that influence regulatory effectiveness in each country.

The analysis focuses solely on legal frameworks that are applicable and went into effect before October 1st, 2024, and regulate fundamental e-governance elements, such as eID, trust services, interoperability, access to and reuse of public sector information, electronic payments, digital communications, data protection, and cybersecurity. The study excludes national procedural legislation governing administrative and judicial processes. It also omits the sectoral legislation governing service delivery across various sectors, such as health, education, social protection, and many others. These regulations, although significant, are excluded because each country has developed its unique service delivery ecosystem.

Due to the absence of globally comparable and methodologically consistent data on citizen uptake of government digital services, particularly outside of the European Union (EU) and the Organisation for Economic Co-operation and Development (OECD), this study adopts a basket of internationally recognised indices to serve as proxies for digital governance performance. These indices collectively capture the availability, quality, and usage of core e-governance systems, offering a multidimensional perspective to triangulate regulatory maturity. Specifically, the E-Government Development Index (EGDI), Digital Identity Readiness Index, Online Service Index (OSI), E-Participation Index (EPI), Open Government Data Index (OGDI), and Global Cybersecurity Index (GCI) were selected because of their relevance and cross-country comparability. Each index captures a key dimension of digital governance: the OSI assesses the availability and usability of online public services; the EPI reflects citizen engagement through digital platforms; the OGDI measures open data transparency; the Digital Identity Readiness Index evaluates the sophistication of national eID systems; and the GCI scores cybersecurity frameworks and institutional capacity. Together, these indicators provide a robust empirical foundation for assessing the real-world implementation and institutional effectiveness of digital governance frameworks.

However, the scope and methodology are not without limitations. The findings are context-specific and may not be universally applicable to all countries. Additionally, the study focuses primarily on regulatory frameworks adopted or applicable on the national level. This approach may not fully capture variations in federal or decentralised governance systems (e.g., Belgium). Nevertheless, the chosen methodology provides a strong foundation for examining the legal frameworks that provide valuable insights from good examples or legislative principles that can enhance the quality of the regulations.

4. Findings and Discussion

This section presents the main findings of the study and explores how the maturity of regulatory frameworks influences the development and implementation of e-governance across the eight countries. The analysis is structured around a three-tier maturity classification: advanced, moderate, and early-stage and is based on the scope of legal frameworks, the operationalisation of key digital enablers, and the degree of public service integration and citizen uptake.

4.1 Maturity Classification

To assess how the depth and operationalisation of legal frameworks influence e-governance performance, this study classifies the eight selected countries into three regulatory maturity categories: advanced, moderate, and early-stage. It is based not on international indices but on a triangulation of legal, institutional, and infrastructural indicators linked to implementing core e-governance components.

Table 2 highlights the classification framework assessing the maturity of regulatory frameworks in e-governance, which is based on three key criteria: (1) *the adoption and scope of legal frameworks*, (2) *the presence and operationalisation of core technical enablers (such as eID, digital signatures, payment systems, notification gateways, and data exchange infrastructure)*, and (3) *the degree of integration and uptake of the online public services*. This classification provided a basis for organising the countries into advanced, moderate, and early-stage maturity groups.

Tab. 2 - Classification criteria for the maturity of regulatory frameworks in e-governance.

Criterion	Advanced	Moderate	Early stage
Regulatory coverage	Comprehensive, up-to-date laws across all key e-governance areas.	Legal instruments adopted for most areas, with some coverage gaps or outdated laws.	Fragmented or partial legal frameworks; significant coverage gaps.
Implementation of key enablers	Fully deployed infrastructure (eID, interoperability, digital services, etc.).	Infrastructure partially rolled out; adoption inconsistent across sectors.	Systems not yet implemented, remain at planning or pilot stages.
Integration and uptake	High levels of citizen engagement, interagency integration, and service use.	Moderate engagement or integration; infrastructure not yet fully utilised.	Low uptake, limited service availability, or minimal system integration.

Based on these criteria, the countries were assessed using evidence from legal documents, institutional arrangements, and available implementation data. This initial classification reflects the degree to which each country's legal frameworks are both comprehensive and operationalised through technical systems and service integration. Belgium, Estonia, and Singapore are classified as having advanced maturity, having adopted comprehensive digital governance frameworks, implemented key enablers, and achieved broad institutional and citizen uptake. Ecuador and Kyrgyzstan fall under the moderate maturity category, having enacted most foundational legal instruments and initiated infrastructure development but still facing gaps in implementation or adoption. Finally, Botswana, Jamaica, and Kenya are considered to be in the early stages of maturity, where legal development remains partial or fragmented, and institutional or infrastructural limitations constrain the operationalisation of technical systems. This classification provides the foundation for the comparative analysis in the sections that follow.

4.2 Regulatory Maturity and Enablers Across Country Contexts

By using the three-tier maturity classification and combining the assessment of the legal-regulatory landscape with the operationalisation of digital enablers, the analysis reveals how regulatory maturity manifests in practice across diverse governance contexts. A comparative summary of key digital enablers is provided in Figure 1, while the e-governance regulatory blueprint of all eight countries is included in the Appendix.

	Belgium	Estonia	Singapore	Ecuador	Kyrgyzstan	Botswana	Jamaica	Kenya
Digital Identity & Trust Services	Belgian eID, CSAM, SigningBox	Smart-ID, Mobile-ID, National eID card	Singpass app, National Digital Identity (NDI).	GOB.EC Mobile ID, FirmaEC digital signature platform	Chip-enabled ID, Unified ID System (ESI), Cloud E-Signature (CEL)	OneGov mobile app	National Identification System (NIDS – not yet operational)	eCitizen Gava Mkononi app
Data Exchange & Interoperability Platforms	BOSA Federal Service Bus (FSB)	X-tee Middleware and Unified eXchange Platform (UXP)	Government Data Architecture (GDA)	SINARDAP Interoperability Platform	Electronic Interoperability Center Tunduk (SMEV)	Not established	Not established	Not established
Digital Payments Infrastructure	Enabled (via eID & eBanking)	Integrated into state systems	Covered under Payment Services Act	Enabled (via integrated public platforms)	Enabled	Enabled	Enabled	Enabled
Secure Digital Messaging	eBox	Government digital inbox	Singpass notifications	Enabled (via GOB.EC and admin e-services)	Enabled (e.g., service portals)	Not established	Not established	Not established
Open Data Portals	data.gov.be	avaandmed.eesti.ee	data.gov.sg	datosabiertos.gob.ec	data.gov.kg	Not established	data.gov.jm	Not established
Data Protection Oversight	Institutional supervision: Belgian Data Protection Authority.	Institutional supervision: Data Protection Inspectorate.	Personal Data Protection Commission Singapore	Superintendent of Data Protection	State Agency for Personal Data Protection	Data Protection Commission	Information Commissioner	Office of the Data Protection Commissioner Kenya
Cybersecurity Coordination Body	Centre for Cyber Security Belgium	National Cyber Security Centre (NCSC-EE)	Cyber Security Agency of Singapore	Cybersecurity Committee under	State Committee for Information Technology and Communications.	Cyber Intelligence Agency	National Cybersecurity Authority (to be established)	Communications Authority of Kenya

Fig. 1 – Key enablers availability in Belgium, Estonia, Singapore, Ecuador, Kyrgyzstan, Botswana, Jamaica and Kenya

Advanced Maturity Contexts: Belgium, Estonia, and Singapore

The three countries classified as having advanced regulatory maturity have enacted comprehensive and coherent legal frameworks across all major pillars of digital governance. These countries illustrate distinct pathways to achieving regulatory maturity: Belgium through federated coordination within an EU-aligned legal framework, Estonia through legal minimalism paired with deep digital integration, and Singapore through centralised, forward-looking regulatory instrumentation.

Belgium has developed a robust and technically advanced legal ecosystem covering eID, trust services, open data, interoperability, cybersecurity, and data protection. As an EU member state, it aligns closely with supranational frameworks such as the eIDAS and General Data Protection Regulation (GDPR). The country's interoperability infrastructure is institutionalised through shared services managed by the Federal Public Service for Policy and Support (BOSA), which coordinates federal and regional implementation. Belgium's national eID is widely adopted and supports authentication, signatures, and secure access across public and private platforms (OECD, 2020c). However, despite its strong legal and technical foundation, Belgium faces persistent horizontal and vertical coordination challenges due to its complex federal structure. While interoperability frameworks are in place, implementation remains uneven across regions, and harmonisation continues to evolve (OECD, 2020c).

Estonia, also and EU member state, represents a highly integrated and centralised digital governance model rooted in a minimalist but enforceable legal framework. Laws such as the Public Information Act, the Cybersecurity Act, and the Digital Signature Act support core national enablers, including eID and the X-Road data exchange platform. These systems enable secure, real-time data sharing among more than 1,000 public and private organisations (Kotka et al., 2016; Krimmer et al., 2021). The legal infrastructure is tightly coupled with Estonia's technological architecture, ensuring flexibility and rapid legislative responsiveness. Over 99% of public services are available online, and citizen uptake is among the highest in the EU (e-Estonia, 2025). Estonia's ability to translate regulatory ambition into operational infrastructure illustrates the value of streamlined legislation that is fully embedded in the digital delivery ecosystem.

Finally, Singapore exemplifies a centralised and anticipatory model of digital governance. Its legal framework spans key areas such as digital identity, cybersecurity, and data governance and is enforced by dedicated agencies like the Cyber Security Agency of Singapore (CSA) and the Personal Data Protection Commission (PDPC). The Singpass system, used by over 4.5 million residents, provides secure, biometric-enabled access to more than 2,000 services across government and private sectors (GovTech Singapore, 2023). Underpinning this architecture are the Government Data Architecture and the Whole-of-Government Application Analytics (WOGAA), which enable interoperable data flows, predictive service delivery, and policy coherence (Smart Nation and Digital Government Office Singapore, 2024). Singapore's Electronic Transactions Act and Cybersecurity Act embody a forward-looking legal orientation that balances innovation with robust enforcement.

Across all three cases, there is a high degree of alignment between legal frameworks, institutional mandates, and technical implementation. These countries score consistently high in international indices such as the EGDI and the OECD's Digital Government Index (OECD, 2020a; UNDESA, 2024). Their experiences demonstrate that regulatory maturity can serve as a key enabler of digital government performance at scale when legal mandates are embedded within strategic governance models and backed by institutional capacity and long-term investment.

These models also highlight the importance of integrating legal clarity with user-centric design, security, and cross-sector coordination.

Moderate Maturity Contexts: Ecuador and Kyrgyzstan

Ecuador and Kyrgyzstan represent countries with moderate regulatory maturity. Both countries have enacted legislation in core areas such as digital identity, data protection, and interoperability and introduced national systems to support digital transformation. However, their regulatory ambition is not yet matched by systemic institutional or technical readiness since both countries face persistent implementation, coordination, and public uptake challenges.

Ecuador has adopted a legal ecosystem that includes legislation on electronic transactions, digital signatures, data protection, and access to public information. These frameworks were largely formalised between 2010 and 2020 and have recently been extended to include provisions for interoperability and digital services. Oversight is provided by institutions such as the Telecommunications Regulation and Control Agency (ARCOTEL) and the Ministry of Telecommunications and the Information Society. Ecuador's technical efforts include the development of a Mobile ID system and a national digital signature platform. However, the practical integration of these enablers into service delivery remains limited. Ministries often operate in silos, with weak horizontal coordination and inconsistent enforcement of legal mandates (Apolo et al., 2020; OECD, 2023).

Ecuador's open data policy, while legally established, also suffers from uneven implementation. Some open government data portals are outdated or non-functional, and usage remains low due to gaps in awareness and infrastructure (World Bank, 2021). Similarly, while digital identity is legally recognised, its application across public services is minimal. These issues are combined by technical fragmentation and digital literacy barriers, especially among underserved populations.

Kyrgyzstan, in contrast, has approached digital governance as part of a broader administrative reform agenda. The country has adopted legal frameworks in digital identity, interoperability, cybersecurity, and data protection. One of its most ambitious initiatives is the Tunduk interoperability platform, which enables data exchange across state agencies and provides a technical backbone for integrated digital services. Tunduk has been internationally recognised as a promising digital enabler (e-Governance Academy, 2021), and some ministries have begun integrating it into their service architecture.

However, the operationalisation of Tunduk remains uneven. While legal structures are in place, enforcement mechanisms are weak, and integration is limited in scope. Regional disparities in institutional capacity and infrastructure continue to hamper consistent service delivery, particularly outside of urban centres (UNDP, 2021). In addition, digital literacy remains a barrier to uptake among citizens, limiting the effectiveness of otherwise functional platforms.

Together, Ecuador and Kyrgyzstan exemplify two distinct but overlapping trajectories within the moderate maturity of digital transformation. Ecuador demonstrates the risks of regulatory advancement without institutional follow-through, while Kyrgyzstan shows how infrastructure can outpace legal enforcement and citizen adoption. Both cases highlight the necessity of aligning legal frameworks with operational readiness, institutional coherence, and public engagement to convert digital ambition into sustainable governance outcomes.

Early-Stage Maturity Contexts: Botswana, Jamaica, and Kenya

Botswana, Jamaica, and Kenya represent countries in the early stages of regulatory maturity, where foundational digital reforms are underway but remain fragmented or underdeveloped. While all three have demonstrated political will and initiated national strategies for digital transformation, their legal frameworks often lack coherence, and operational enablers are either nascent or inconsistently implemented. These countries reflect distinct entry points into digital governance: Botswana through cautious regulatory rollout, Jamaica through identification-led reform, and Kenya through platform-driven service expansion without fully consolidated legislation.

Botswana has focused on incremental digital reforms, adopting key legislation such as data protection laws and developing strategic frameworks like the National ICT Policy (Maitlamo). However, critical legal instruments covering digital identity, trust services, interoperability, and secure digital communication are either missing or remain in preliminary stages. The SmartBots initiative has aimed to digitise selected public services, but institutional fragmentation and limited central oversight have slowed broader implementation (Government of Botswana, 2021; UNECA, 2023). Digital ID systems are still in pilot phases, and inter-agency coordination is weak. Open data practices are emerging but suffer from low levels of proactive disclosure and limited availability in machine-readable formats (Ndlovu, 2024). Botswana illustrates a legal and institutional environment that is evolving but lacks the depth and cohesion required for integrated digital governance.

Jamaica has taken a more targeted legislative approach centred on its Data Protection Act (2020) and the phased rollout of the National Identification System (NIDS). These initiatives form the backbone of Jamaica's legal architecture for digital governance, aiming to support secure, identity-based service delivery. However, enabling frameworks for interoperability, trust services, and digital signatures remain underdeveloped or unimplemented. The 2019 Supreme Court ruling, which declared the original NIDS legislation unconstitutional due to privacy concerns, highlighted public mistrust and the need for more robust legal safeguards (Caribbean Policy Research Institute (CAPRI), 2020). Although institutions like the Office of the Information Commissioner exist, they often operate with evolving mandates and limited capacity. Open data initiatives remain sporadic, with most public data either unpublished or not structured for reuse. Jamaica's experience underscores the importance of aligning legal reform with institutional capability and sustained public engagement to build trust and support uptake.

Lastly, Kenya presents a more complex but equally instructive case. The country has launched eCitizen, a major digital portal offering over 5,000 public services, and enacted the Data Protection Act (2019), positioning itself as a regional leader in service digitisation. However, its regulatory framework remains fragmented, with overlapping mandates across agencies and laws covering interoperability, trust services, and digital signatures (CIPESA, 2022; Nyangena et al., 2021). Efforts to introduce national digital ID systems, including Huduma Namba and the more recent Maisha Namba, have faced legal setbacks and public criticism over data protection and exclusion risks. Huduma Namba was suspended by the High Court in 2021 due to inadequate legislative safeguards (Njoya, 2023), and Maisha Namba has encountered similar pushback over insufficient consultation and transparency (Kennedy, 2025). Despite rapid service digitisation, Kenya's experience illustrates that platform expansion without legal and institutional consolidation can undermine public trust and impede sustainable progress.

Taken together, these cases highlight the vulnerabilities of early-stage digital governance contexts. While political support for digital reform exists, legal gaps, institutional fragmentation, and low levels of citizen trust hinder the full operationalisation of enablers. Early-stage countries risk uneven progress and increase the digital divide gap without targeted investment in comprehensive legal frameworks, coordinated governance structures, and public trust-building measures. These findings reinforce the importance of treating regulatory maturity not only as a legislative exercise but as a multidimensional condition grounded in institutional readiness, operational infrastructure, and societal inclusion.

4.3 Cross-Cutting Patterns and Performance Validation

This section synthesises key insights from the previous country analyses by examining how regulatory maturity correlates with broader digital governance outcomes. It shifts from country-level narratives to a more aggregated, cross-case perspective using internationally recognised indicators and longitudinal data. The aim is to empirically validate the maturity classification and identify common drivers and limitations of successful digital transformation.

Empirical Validation through Global Indices

To complement the maturity framework and deepen comparative insights, this section draws on five internationally recognised indices: the Digital Identity Readiness Index, OSI, EPI, OGDI, and the GCI. These indicators capture the operational capacity of digital systems across dimensions such as infrastructure, service availability, citizen engagement, data openness, and cybersecurity. Table 3 summarises country scores across these dimensions.

Tab. 3 – Relevant indicators (Global Digital Identity Index, 2024; ITU, 2024; UNDESA, 2024).

Indicator	BE	BW	EC	EE	JM	KE	KG	SG
Digital Identity Readiness Index	84	54.85	58.02	77.5	33.95	50.43	78.11	81.5
Online Service Index	0.72	0.40	0.89	0.99	0.57	0.78	0.60	0.98
E-Participation Index	0.50	0.27	0.88	0.96	0.44	0.52	0.47	0.96
Open Government Data Index	0.85	0.46	0.85	1.00	0.56	0.59	0.54	1.00
Global Cybersecurity Index	96.81	78.60	87,18	96,04	58.20	98.59	65.59	99.86

The indicators generally reinforce the maturity groupings outlined in Section 4.2. Advanced countries, Belgium, Estonia, and Singapore consistently score high across all categories. Estonia and Singapore are especially strong in service integration and digital ID, while Belgium performs well on open data and cybersecurity. These results illustrate that institutionalised legal frameworks when paired with operational infrastructure, predict stronger e-governance performance. On the other hand, moderate countries, such as Ecuador and Kyrgyzstan, display more uneven profiles. Ecuador performs relatively well in online services and open data, reflecting its emphasis on front-end platforms but scores lower in cybersecurity and institutional coherence. Kyrgyzstan performs comparatively better in digital ID, partly due to the Tunduk platform, but lags in service integration and infrastructure. Finally, early-stage countries, Botswana, Jamaica, and Kenya, generally score lower across most indices. Kenya stands out slightly with a higher GCI score, indicating relative strength in cybersecurity institutions, but remains behind in legal coherence and service integration. These patterns reinforce the broader argument that while legislative reform is a necessary condition, it is insufficient without robust institutions, systems, and citizen trust.

Longitudinal Trends in the EGDI

In addition to cross-sectional comparisons, the E-Government Development Index (EGDI) provides a longitudinal view of each country's trajectory between 2014 and 2024 (Figure 2).

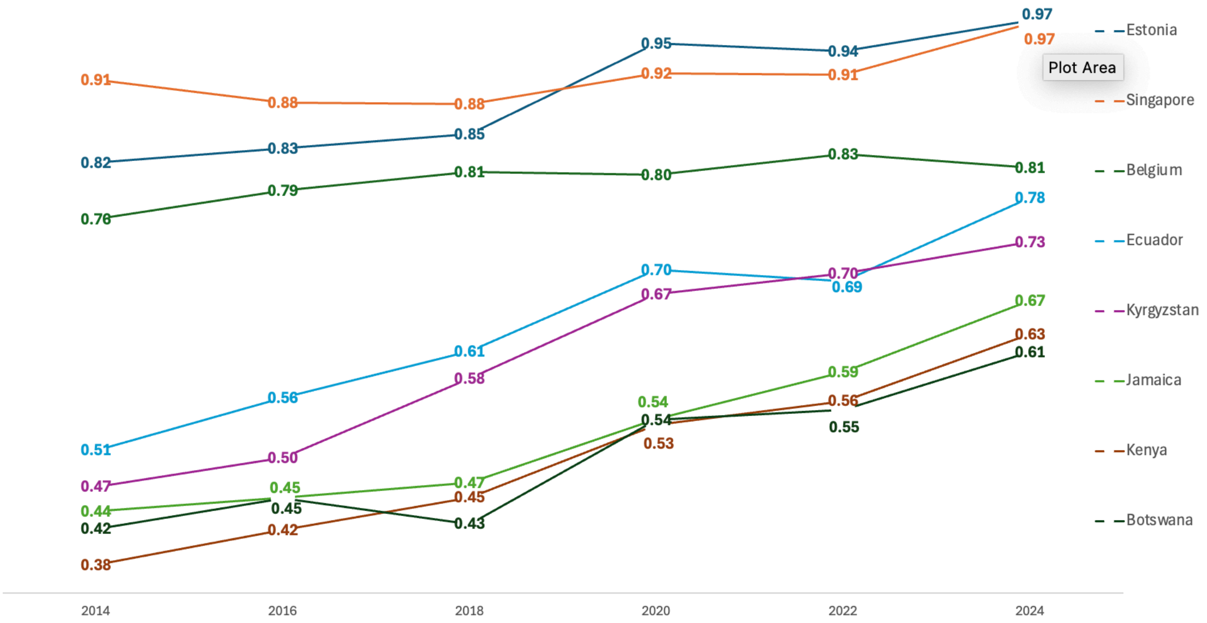

Fig. 2 – E-Government Development Index 2014-2024 (UNDESA, 2025).

Evidently, Estonia and Singapore show sustained progress, with Estonia increasing from 0.85 to 0.97 and Singapore maintaining consistently high scores. These gains are tied to iterative legal updates and investments in whole-of-government architectures. Moderate countries, such as Ecuador and Kyrgyzstan, have demonstrated steady improvement. Ecuador increased from 0.51 to 0.78, supported by platform expansion and external technical assistance. Kyrgyzstan rose from 0.47 to 0.73, reflecting the impact of institutional innovation, policy borrowing, and the rollout of Tunduk.

In contrast, early-stage countries show slower or inconsistent gains. Kenya improved from 0.38 to 0.63 due to its expanding service platforms, but progress is constrained by institutional fragmentation. Botswana and Jamaica exhibit only marginal growth, illustrating the limitations of uncoordinated or under-resourced reform. Interestingly, while classified as advanced, Belgium shows only modest growth (0.76 to 0.81), suggesting that decentralised governance may impede long-term progress despite early regulatory leadership.

Key Cross-Cutting Patterns

Three overarching insights emerge from the cross-country synthesis:

- **Legal frameworks are foundational but insufficient without institutional suppor**t: Advanced countries show that comprehensive legal frameworks embedded in operational systems, such as Estonia's X-Road and eID, enable secure data flows and cross-sector integration (Kotka et al., 2016; Krimmer et al., 2021). However, moderate countries like Ecuador and Kyrgyzstan reveal that legal adoption without enforcement, capacity, and uptake delivers limited outcomes (Bannister & Connolly, 2011b; OECD, 2023). This confirms existing research suggesting that the mere existence of laws does not guarantee compliance or transformation unless supported by enforcement mechanisms and institutional readiness (Bannister & Connolly, 2011b; Jordanoski & Meyerhoff Nielsen, 2023).

- **Institutional capacity and infrastructure determine the impact of regulation**: The implementation gap is widest in moderate and early-stage contexts. Ecuador's legal basis for interoperability is undermined by fragmented governance (Apolo et al., 2020), while Kyrgyzstan's infrastructure investments remain underutilised (UNDP, 2021). By contrast, advanced countries pair regulation with long-term investments in technical and organisational infrastructure (Heeks, 2008). This supports the argument that regulatory maturity must be paired with governance capacity and adequate financing to deliver meaningful digital outcomes (OECD, 2020b).

- **Regulatory maturity is closely linked to interoperability and service integration**: Countries with legal mandates for data exchange and authentication, like Estonia and Belgium, show high levels of integration and service coherence (Bruijn, 2021; Kotka et al., 2016). These frameworks are embedded into public administration, enabling seamless, cross-agency services. In early-stage contexts, the absence of such frameworks leads to siloed systems and duplicative service delivery, limiting scalability and trust (Dovhan et al., 2022; Wimmer et al., 2018).

These findings confirm that regulatory maturity is a strong predictor of e-governance performance but not a guarantee. Countries with established legal frameworks and well-embedded digital enablers consistently outperform those where reform remains fragmented or under-resourced. This cross-cutting synthesis reinforces the value of legal-regulatory maturity as a diagnostic lens while highlighting the risks of symbolic compliance in contexts where enforcement and technical infrastructure are lacking.

4.4 From Regulation to Realisation: Barriers to Effective Implementation

While regulatory maturity is a critical enabler of digital governance, it does not, on its own, guarantee meaningful implementation. Across the eight countries studied, several cross-cutting constraints continue to obstruct the translation of legal frameworks into operational digital ecosystems. These barriers underscore the need for a holistic approach that aligns legal ambition with institutional capacity, infrastructure readiness, and societal inclusion. These include:

- **Legal and Institutional Misalignment:** One of the most persistent challenges is fragmented governance and siloed legal mandates. In countries such as Kenya and Botswana, overlapping responsibilities and weak inter-ministerial coordination have delayed the adoption of shared platforms and hindered the enforcement of national digital strategies. Ecuador faces similar issues, where the lack of vertical alignment between national and subnational regulations has resulted in duplicative efforts and inefficiencies. These patterns reflect broader structural weaknesses, where legal reforms are not sufficiently supported by inter-agency collaboration or clearly defined institutional mandates (Nyman-Metcalf, 2014; OECD, 2020a).

- **Operational and Infrastructure Gaps:** Digital transformation also hinges on robust infrastructure and sustainable investment. In many early-stage countries, inadequate digital infrastructure, such as limited connectivity, fragmented identity systems, or insecure data hosting environments, impairs the rollout of legally mandated systems. Botswana and Kenya exemplify this dynamic, where the technical infrastructure lags behind strategic plans. Even where policies are well-articulated, their implementation is often delayed due to fiscal constraints or reliance on donor funding. Without adequate financing and a long-term maintenance strategy, legal frameworks risk becoming aspirational rather than actionable (OECD, 2020b).

- **Societal Readiness and Trust:** Even the most coherent legal and technical systems depend on societal trust and digital literacy to gain traction. In Jamaica, for instance, the National Identification System (NIDS), though legally established, has faced significant public opposition due to privacy concerns and insufficient consultation. (Caribbean Policy Research Institute (CAPRI), 2020) Similarly, Kenya's Huduma Namba and Maisha Namba initiatives were suspended or contested on legal grounds, with civil society raising concerns over exclusion risks and inadequate data safeguards (Kennedy, 2025; Njoya, 2023). These examples underscore that institutional design must be coupled with public engagement and transparent governance. Without these elements, uptake remains low, and compliance is limited even in legally sound systems (Grigorescu et al., 2016; Sanjay Jadhav, 2023).

Finally, across all maturity levels, governments face growing difficulties in responding to rapid technological change. While Singapore has begun adapting its legal frameworks to accommodate emerging technologies such as AI and fintech, most countries remain reactive, contributing to regulatory lag and oversight gaps (Firdaus et al., 2024; OECD, 2020b). This mismatch between innovation cycles and legislative evolution highlights the need for more agile, anticipatory regulatory design.

5. Conclusion and Future Work

This paper examined how the maturity of regulatory frameworks correlates with the development of e-governance across a diverse set of countries. While regulatory frameworks are indispensable for enabling secure, efficient, and resilient digital government systems, their effectiveness depends on broader structural and institutional conditions. The findings confirm that legal design alone is insufficient unless matched by operational capacity, coordinated governance, and public engagement. As digital transformation accelerates globally, the ability of governments to align legal innovation with institutional capacity and societal needs will remain a decisive factor in shaping the future of digital public administration.

Drawing from a cross-case comparative analysis of eight jurisdictions, the findings confirm that comprehensive, coherent, and enforceable regulatory environments are closely associated with more advanced e-governance outcomes. Countries with mature legal systems, such as Belgium, Estonia, and Singapore, have successfully implemented key digital enablers, achieved high levels of interoperability, and fostered institutional and citizen trust in digital services. This conclusion is further supported by comparative analysis using internationally recognised indicators, which offer empirical validation of the observed regulatory maturity classifications. In contrast, jurisdictions with fragmented or underdeveloped regulatory frameworks face persistent challenges related to implementation, enforcement, and scalability. These barriers, ranging from legal fragmentation to enforcement gaps and infrastructure constraints, demonstrate the need for regulatory maturity to be understood as both a legal and operational condition.

This research introduces an empirically grounded, three-tier classification of regulatory maturity (advanced, moderate, and early-stage) based on legal scope, system operationalisation, and institutional integration. By combining qualitative analysis with internationally recognised indicators (e.g., EGDI, OSI, EPI, GCI), the study offers a replicable framework for diagnosing regulatory readiness across diverse national contexts. It also serves as a practical benchmarking tool for policymakers, enabling the identification of regulatory gaps and supporting targeted reforms aligned with national capabilities and digital ambitions.

Future research could extend this analysis by examining the influence of global and regional legal frameworks, such as the EU's eIDAS, GDPR, and NIS2, the OECD's digital governance principles, or emerging global standards on Artificial Intelligence, in shaping domestic regulatory ecosystems. Also, further work could examine the effects of regulatory design at subnational or federal levels, particularly in countries with decentralised governance structures, such as Belgium, Australia, or India. Longitudinal studies could also help clarify how legal frameworks adapt to technological change and whether regulatory evolution leads to sustained governance outcomes. Understanding how legal frameworks evolve over time and how they respond to emerging technologies will be essential for designing future-ready digital governance systems.

Acknowledgement

- **Funding or Grant:** This document is a result of the project "INOV.EGOV-Digital Governance Innovation for Inclusive, Resilient and Sustainable Societies / NORTE-01-0145-FEDER-000087", supported by the Norte Portugal Regional Operational Programme (NORTE 2020), under the PORTUGAL 2020 Partnership Agreement, through the European Regional Development Fund (EFDR).
- **Conflict Of Interest (COI)***: There is no conflict of interest.

References

Apolo, D., Melo, M., Solano, J., & Aliaga-Sáez, F. (2020). Pending issues from digital inclusion in Ecuador: challenges for public policies, programs and projects developed and ICT-mediated teacher training. *Digital Education Review*, *37*, 130–153. https://doi.org/10.1344/der.2020.37.130-153

Bannister, F., & Connolly, R. (2011a). *Transformation and public sector values*. na.

Bannister, F., & Connolly, R. (2011b). Trust and transformational government: A proposed framework for research. *Government Information Quarterly*, *28*(2), 137–147. https://doi.org/10.1016/j.giq.2010.06.010

Bruijn, H. (2021). *The Governance of Privacy: Privacy as Process: The Need for Resilient Governance*. https://doi.org/10.5117/9789463729673

Caribbean Policy Research Institute (CAPRI). (2020). *Who am I? The People dem NIDS*.

Chatterjee, S., & N.S., S. (2022). Artificial intelligence and human rights: a comprehensive study from Indian legal and policy perspective. *International Journal of Law and Management*, *64*(1), 110–134. https://doi.org/10.1108/IJLMA-02-2021-0049

Chauhan, R., Estevez, E., & Janowski, T. (2008). A model for policy interventions in support of electronic governance. *Proceedings of the 2nd International Conference on Theory and Practice of Electronic Governance*, 199–205. https://doi.org/10.1145/1509096.1509135

CIA.gov. (2025). *The World Factbook*. Https://Www.Cia.Gov/the-World-Factbook/.

CIPESA. (2022). *State of Freedom. in Afraica*.

Cordella, A., & Bonina, C. M. (2012). A public value perspective for ICT enabled public sector reforms: A theoretical reflection. *Government Information Quarterly*, *29*(4), 512–520. https://doi.org/10.1016/j.giq.2012.03.004

Dovhan, V., Yunyk, I., Kurchyn, O., Zhupnyk, V., & Moskalenko, S. (2022). Building Legal Mechanisms for Electronic Governance Development. *Cuestiones Políticas*, *40*(73), 172–191. https://doi.org/10.46398/cuestpol.4073.08

e-Estonia. (2025). *e-Estonia: Facts & Figures*. Https://E-Estonia.Com/Facts-and-Figures/.

e-Governance Academy. (2021). *Supporting Service-Oriented e-Government Interoperability*.

Firdaus, D. U. F. binti, Roslan, N. A. bin, Saferdin, W. F. H. binti W. M., Zulkarnain, I. F. binti, & Samasu, N. F. binti. (2024). AI Integration in Malaysian Public Administration for Improved Governance. *International Journal of Research and Innovation in Social Science*, *VIII*(IX), 3799–3812. https://doi.org/10.47772/IJRISS.2024.8090316

Franco, F. S. R. (2024). Brazilian Federal Public Administration, open data, technologies and the right to Information. *Brazilian Journal of Law, Technology and Innovation*, *2*(1), 140–192. https://doi.org/10.59224/bjlti.v2i1.140-192

Gil-Garcia, J. R., Dawes, S. S., & Pardo, T. A. (2018). Digital government and public management research: finding the crossroads. *Public Management Review*, *20*(5), 633–646. https://doi.org/10.1080/14719037.2017.1327181

Global Digital Identity Index. (2024). *Digital Identity Readiness Index*. Https://Digitalidentityindex.Com.

González, L., Echevarría, A., Morales, D., & Ruggia, R. (2016). An E-government Interoperability Platform Supporting Personal Data Protection Regulations. *CLEI Electronic Journal*. https://doi.org/10.19153/cleiej.19.2.7

Government of Botswana. (2021). *SmartBots*. Https://Smartbots.Gov.Bw.

GovTech Singapore. (2023). *Singpass and National Digital Identity Statistics*.

Gregory, J. (2002). Solving Legal Issues in Electronic Government: Jurisdiction, Regulation, Governance. *Canadian Journal of Law and Technology*, *1*(3).

Grigorescu, A., Lupu, M.-M., Iancu, A. A., Tuca, M. V., Vatamatescu, M. E., Andrei, A. G., Daniel, P., Săvulescu, C., Iordache, L., Dincă, D. V., Antonovici, C. G., Dumitrescu, A., Dumitru, B. D., Popescu, M.-L., & Popa, F. (2016). *Comparative Public Administration and Management – Good Governance and Regulatory Quality in the 21st Century*. https://api.semanticscholar.org/CorpusID:155423230

Hasan, M. M., Anagnostopoulos, D., Kousiouris, G., Stamati, T., Loucopoulos, P., & Nikolaidou, M. (2019). An Ontology based Framework for E-Government Regulatory Requirements Compliance. *International Journal of E-Services and Mobile Applications*, *11*(2), 22–42. https://doi.org/10.4018/IJESMA.2019040102

Hasan, M. M., Loucopoulos, P., Anagnostopoulos, D., & Nikolaidou, M. (2015). Regulatory requirements compliance in e-Government service development. *2015 18th International Conference on Computer and Information Technology (ICCIT)*, 254–259. https://doi.org/10.1109/ICCITechn.2015.7488078

He, Z. (2011). The Legal Regulations of E-Government. *2011 International Conference on Management and Service Science*, 1–4. https://doi.org/10.1109/ICMSS.2011.5999430

Heeks, R. (2002). *Reinventing Government in the Information Age* (R. Heeks, Ed.). Routledge. https://doi.org/10.4324/9780203204962

Heeks, R. (2008). eGovernment for development: Success and Failure in eGovernment Projects. *Institute for Development Policy and Management (IDPM), University of Manchester. Http://Www. Egov4dev. Org/Egovdefn. Htm*.

ITU. (2024). *Global Cybersecurity Index 2024*.

ITU. (2025). *DataHum*. Https://Datahub.Itu.Int.

Jordanoski, Z., & Meyerhoff Nielsen, M. (2023). The challenge of web accessibility: an evaluation of selected government websites and service portals of high, middle and low-income countries. *Proceedings of the 16th International Conference on Theory and Practice of Electronic Governance*, 101–110. https://doi.org/10.1145/3614321.3614343

Kennedy, C. (2025, March 13). *Legal Challenge Targets Kenya's New Digital ID System Over Rights Concerns*.

Korvat, O. (2023). Development of Electronic Governance to a Digital Ecosystem. *Law and Innovations*, *2 (42)*, 41–45. https://doi.org/10.37772/2518-1718-2023-2(42)-5

Kotka, T., del Castillo, C. I. V. A., & Korjus, K. (2016). Estonian e-Residency: Benefits, Risk and Lessons Learned. In A. Kő & E. Francesconi (Eds.), *Electronic Government and the Information Systems Perspective* (pp. 3–15). Springer International Publishing.

Krimmer, R., Dedovic, S., Schmidt, C., & Corici, A.-A. (2021). Developing Cross-border E-Governance: Exploring Interoperability and Cross-border Integration. In N. Edelmann, C. Csáki, S. Hofmann, T. J. Lampoltshammer, L. Alcaide Muñoz, P. Parycek, G. Schwabe, & E. Tambouris (Eds.), *Electronic Participation* (pp. 107–124). Springer International Publishing.

Lebid, O. (2021). E-governance of the economy of the future: world experience and prospects of Ukraine. *Ekonomika APK*, *324*(10), 98–110. https://doi.org/10.32317/2221-1055.202110098

López-López, V., Iglesias-Antelo, S., Vázquez-Sanmartín, A., Connolly, R., & Bannister, F. (2018). e-Government, Transparency &amp; Reputation: An Empirical Study of Spanish Local Government. *Information Systems Management*, *35*(4), 276–293. https://doi.org/10.1080/10580530.2018.1503792

Luna-Reyes, L. F., Picazo-Vela, S., Luna, D. E., & Gil-Garcia, J. R. (2016). Creating Public Value through Digital Government: Lessons on Inter-Organizational Collaboration and Information Technologies. *2016 49th Hawaii International Conference on System Sciences (HICSS)*, 2840–2849. https://doi.org/10.1109/HICSS.2016.356

Mahrer, H., & Krimmer, R. (2005). Towards the enhancement of e-democracy: identifying the notion of the ‘middleman paradox.’ *Information Systems Journal*, *15*(1), 27–42. https://doi.org/10.1111/j.1365-2575.2005.00184.x

Meyerhoff Nielsen, M. (2017). eGovernance frameworks for successful citizen use of online services: A Danish-Japanese comparative analysis. *JeDEM - EJournal of EDemocracy and Open Government*, *9*(2), 68–109. https://doi.org/10.29379/jedem.v9i2.462

Meyerhoff Nielsen, M., & Jordanoski, Z. (2020). Digital transformation, governance and coordination models: A comparative study of Australia, Denmark and the Republic of Korea. *The 21st Annual International Conference on Digital Government Research*, 285–293. https://doi.org/10.1145/3396956.3396987

Meyerhoff Nielsen, M., & Krimmer, R. (2015). *Reuse of Data for Personal and Proactive Service: An Opportunity Not Yet Utilised.*

Muliaro Wafula, J. (2012). *ICT Policy and Strategies: Towards E-Governance and Sustainable Development: The Case of East African Community and Kenya.* https://api.semanticscholar.org/CorpusID:109059170

Mustafa, G., Rafiq, W., Jhamat, N., Arshad, Z., & Rana, F. A. (2025). Blockchain-based governance models in e-government: a comprehensive framework for legal, technical, ethical and security considerations. *International Journal of Law and Management*, *67*(1), 37–55. https://doi.org/10.1108/IJLMA-08-2023-0172

Navarra, D., & Cornford, T. (2003). *A Policy Making View of E-Government Innovations in Public Governance.*

Ndlovu, T. (2024). Botswana showcases e-government’s privacy pitfalls Ndlovu. *Digital Rights Southern Africa*, *2*, 6–11.

Njoya, S. (2023, December 7). Kenya: High Court Suspends Digital ID, Citing Data Protection Concerns. *Https://Www.Wearetech.Africa/En/Fils-Uk/News/Tech/Kenya-High-Court-Suspends-Digital-Id-Citing-Data-Protection-Concerns*.

Nyangena, J., Rajgopal, R., Ombech, E. A., Oloo, E., Luchetu, H., Wambugu, S., Kamau, O., Nzioka, C., Gwer, S., & Ndiritu Ndirangu, M. (2021). Maturity assessment of Kenya’s health information system interoperability readiness. *BMJ Health & Care Informatics*, *28*(1), e100241. https://doi.org/10.1136/bmjhci-2020-100241

Nyman-Metcalf, K. (2014). e-Governance in Law and by Law. In T. Kerikmäe (Ed.), *Regulating eTechnologies in the European Union: Normative Realities and Trends* (pp. 33–51). Springer International Publishing. https://doi.org/10.1007/978-3-319-08117-5_3

OECD. (2020a). *Digital Government Index*. https://doi.org/10.1787/4de9f5bb-en

OECD. (2020b). *Going Digital integrated policy framework*. https://doi.org/10.1787/dc930adc-en

OECD. (2020c). *OECD Development Co-operation Peer Reviews: Belgium 2020*. OECD. https://doi.org/10.1787/026f1aad-en

OECD. (2020d). *The OECD digital government policy framework*. https://doi.org/10.1787/f64fed2a-en

OECD. (2023). *Digital Government Review of Latin America and the Caribbean*. OECD. https://doi.org/10.1787/29f32e64-en

Okon, S. U. (2024). Enhancing Transparency and Accountability in Public Service through Open Data Initiatives: Insights from Estonia and Policy Recommendations for the United States. *Asian Journal of Economics, Business and Accounting*, *24*(9), 328–349. https://doi.org/10.9734/ajeba/2024/v24i91496

Ortega, E., Tran, M., & Bandeen, G. (2023). AI Digital Tool Product Lifecycle Governance Framework through Ethics and Compliance by Design†. *2023 IEEE Conference on Artificial Intelligence (CAI)*, 353–356. https://doi.org/10.1109/CAI54212.2023.00155

Papadopoulos, T., & Kanellis, P. (2012). *Public Sector Reform Using Information Technologies*. IGI Global. https://doi.org/10.4018/978-1-60960-839-2

Park, S., Kim, S., Kim, B., Kim, D., & Kwon, H. (2016). Characteristics of the Legal Framework of Korea in the Age of Data and Looking Forward - from Media Theory Point of View. *International Journal of Software Engineering and Its Applications*, *10*(5), 109–124. https://doi.org/10.14257/ijseia.2016.10.5.11

Rohlfing, I. (2012). *Case Studies and Causal Inference: An Integrative Framework*. https://api.semanticscholar.org/CorpusID:117082449

Sanjay Jadhav, S. (2023). Impact of the Right to Information Act by Regulating Transparency in Corruption of India. *International Journal of Science and Research (IJSR)*, *12*(2), 285–290. https://doi.org/10.21275/MR23129125420

Schneider, J.-P., Erny, J., & Enderlein, F. (2024). Collaborative Governance Structures for Interoperability in the EU's new data acts. *European Journal of Risk Regulation*, 1–12. https://doi.org/10.1017/err.2024.46

Shkarlet, S., Oliychenko, I., Dubyna, M., Ditkovska, M., & Zhovtok, V. (2020). Comparative analysis of best practices in e-Government implementation and use of this experience by developing countries. *Administratie Si Management Public*, *34*, 118–136. https://doi.org/10.24818/amp/2020.34-07

Smart Nation and Digital Government Office Singapore. (2024). *Smart Nation 2.0: A Thriving Digital Future for All*.

Thornberg, R. (2012). Informed Grounded Theory. *Scandinavian Journal of Educational Research*, *56*(3), 243–259. https://doi.org/10.1080/00313831.2011.581686

Tojiev, O. (2024). Laying the legal groundwork for digital governance. *International Journal of Law, Justice and Jurisprudence*, *4*(1), 06–08. https://doi.org/10.22271/2790-0673.2024.v4.i1a.86

UNDESA. (2022). *UN E-Government Survey 2022*.

UNDESA. (2024). *UN E-Government Survey 2024*.

UNDESA. (2025). *UN E-Government Knowledge*. Https://Publicadministration.Un.Org/Egovkb/En-Us/Data-Center.

UNDP. (2021). *Entry points for digital transformation in Kyrgyzstan*.

UNECA. (2023). *Botswana Establishes SmartBots Lab to Drive Innovation and Digital Transformation*. Https://Www.Uneca.Org/Stories/Botswana-Establishes-Smartbots-Lab-to-Drive-Innovation-and-Digital-Transformation.

Veit, D., & Huntgeburth, J. (2014). Legal Aspects of Digital Service Delivery. In D. Veit & J. Huntgeburth (Eds.), *Foundations of Digital Government: Leading and Managing in the Digital Era* (pp. 51–66). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-38511-7_4

Wimmer, M. A., Boneva, R., & di Giacomo, D. (2018). Interoperability governance: a definition and insights from case studies in Europe. *Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age*. https://doi.org/10.1145/3209281.3209306

World Bank. (2021). *Digital Government Readiness Assessment (DGRA) toolkit*.

Yin, R. K. (2017). *Case Study Research and Applications: Design and Methods* (Sixth). SAGE Publications.

Appendix

Tab. – E-Governance Regulatory Landscape in Belgium, Estonia, Singapore, Ecuador, Kyrgyzstan, Botswana, Jamaica and Kenya.

	Belgium	Estonia	Singapore	Ecuador	Kyrgyzstan	Botswana	Jamaica	Kenya
eID and Trust services	Regulation (EU) No 910/2014 (eIDAS Regulation); Regulation (EU) 2024/1183 (eIDAS 2.0)		Electronic Transactions Act	Law for the Digital and Audiovisual Transformation and its General Regulations; Law on Identity and Civil Data Management; Administrative Code; Law on Electronic Commerce, Signature and Data Messages.	Law on Electronic Governance; Law about Electronic Signature; Regulation on the Unified Identification System.	National Registration Act; Electronic Communication and Transaction Act; Electronic Records (Evidence) Act and Regulations.	National Identification and Registration Act (NIRA); Electronic Transactions Act.	Information and Communications Act; Electronic Certification and Domain Name Administration Regulation; Registration of Persons Act; Regulations and Data Protection Regulations.
	Law relating to population registers, identity cards, ...; Law on Electronic Identification.	Identity Documents Act; Electronic Identification and Trust Services for Electronic Transactions Act.						
Interoperability & Data Exchange	Regulation (EU) 2024/903 (Interoperable Europe Act); European Interoperability Framework.		Public Sector Governance Act (PSGA); Government Data Architecture (GDA).	Law of the National System of Public Data Registrations; Interoperability Guidelines in the Executive Function, Technical Standard for Interoperability Public Data Registries; Government Interoperability Technical Standard.	Law on E-Governance; Decree on the Requirements for the interaction of information systems in the Electronic Interaction System Tunduk.	No regulation	No regulation (only PSG Manual (ICT Policies, Standards & Guidelines)	No regulation (only Government Enterprise Architecture Framework)
	Law … on establishing an Infrastructure for Spatial Information in the European Community (INSPIRE); Law guaranteeing the principle of a single collection of data...; Belgium Interoperability Framework (Belgif).	Public Information Act; Regulation on Exchange Layer of Information System (X-Road); Estonian Interoperability Framework.						
E-payments	EU Directive 2015/2366 (Payment Services Directive (PSD2)		Payment Services Act	Law on Electronic Commerce, Signature and Data Messages.	Law on the payment system.	Electronic Communication and Transaction Act	Electronic Transactions Act	Information and Communications Act
	Law on the statute and supervision of payment institutions and electronic money institutions…	Administrative Procedure Act; Payment Institutions and Electronic Money Institutions Act.						
Digital Post	Law on Electronic Communications	Administrative Procedure Act	Electronic Transactions Act; Public Sector Governance Act (PSGA).	Law for the Optimisation and Efficiency of Administrative Procedures; Law on E-Commerce, Signature and Data Messages.	Law on E-Governance; Administrative-Procedure Code; Decree on Urgent Measures to Enhance the Implementation of Digital Technologies in Public Administration.	Electronic Communication and Transaction Act	Electronic Transactions Act	Information and Communications Act
Access to and reuse of Public Sector Information	Regulation (EU) 2018/1724 (Single Digital Gateway Regulation); Regulation (EU) 2018/1807 (free flow of non-personal data across the EU); Regulation (EU) 2022/868 (Data Governance Act).		No regulation	Law on Transparency and Access to Public Information and Open Data Policy.	Law on Guarantees and Freedom of Access to Information; Law about access to information held by state bodies and local self-government bodies.	Freedom of Information Bill	Access to Information Act Open Data Policy.	Access to Information Act
	Law on the Right of Access to Administrative Documents; Law on the Reuse of Public Sector Information	Public Information Act						
Data Protection	Regulation (EU) 2016/679 (General Data Protection Regulation (GDPR))		Personal Data Protection Act; Public Sector Governance Act (PSGA); Spam Control Act.	Law on the Protection of Personal Data	Law about personal information	Data Protection Act	Data Protection Act	Data Protection Act
	Law on establishing the Data Protection Authority; Law on the Protection of Private Life with regard to the Processing of Personal Data.	Personal Data Protection Act						
Cybersecurity	Regulation (EU) 2019/881 (EU Cybersecurity Act); EU Directive 2022/2555 (Network and Information Security Directive (NIS2))		Computer Misuse Act; Cybersecurity Act; Instruction Manual for Infocomm Technology and Smart Systems (ICT&SS) Management.	Penal Code; Cybersecurity Policy.	Law on the protection of state secrets n.210; Decree on the Requirements for the protection of information contained in databases of state information systems n. 762.	Cybercrime and Computer-Related Crimes Act	Cybercrimes Act	Information and Communications Act; Computer Misuse and Cybercrimes Act.
	Law on the Establishment of a Security Framework for Information Systems Having General Interest	Cybersecurity Act						