

Technology, State Capacity and Digital Inclusion: Explaining Divergent Pathways of Digital Governance in Estonia, India and Kenya

MANU THOMAS & AJITHA S.

University of Kerala

The rapid diffusion of digital technologies is reshaping public administration by transforming service delivery, administrative processes, and citizen–state interactions. However, technological adoption does not necessarily produce effective or inclusive digital governance; its outcomes are mediated by state capacity, institutional arrangements, regulatory frameworks, and patterns of digital inclusion. This study comparatively examines the divergent pathways of digital governance in Estonia, India, and Kenya, conceptualised respectively as a trust-based digital state, a state-led Digital Public Infrastructure (DPI) model, and a market-driven digital ecosystem. Drawing on state capacity, institutional legitimacy, and digital inclusion as an analytical framework, the study employs a qualitative comparative analysis based on secondary data from academic literature, government documents, and reports of international organisations. The findings demonstrate that differences in institutional capacity, regulatory effectiveness, public trust, and access to digital infrastructure significantly shape digital governance outcomes. Estonia illustrates how institutional trust, interoperable digital infrastructure, and strong regulatory capacity can support a highly integrated digital state. India demonstrates the transformative potential of large-scale DPI while also revealing challenges related to institutional capacity, unequal access, and inclusion. Kenya highlights the role of private-sector innovation and mobile-based digital services, alongside persistent regulatory and infrastructural constraints. The study argues that digital transformation is not technologically deterministic but institutionally conditioned: similar technologies generate divergent governance outcomes when embedded in different political, regulatory, and socio-economic contexts. The comparative analysis contributes to the literature on digital governance by demonstrating that state capacity, legitimacy, and digital inclusion are mutually reinforcing conditions for translating technological innovation into effective, accountable, and inclusive governance.

Keywords: Digital Governance; State Capacity; Digital Inclusion; Legitimacy; Digital Public Infrastructure; Comparative Governance; Artificial Intelligence

Introduction

The introduction of Information and Communication Technologies (ICT) has transformed governance. Digital technologies like artificial intelligence, blockchain, big data analytics, machine learning and mobile platforms have led to rapid transformation in administration. Governments worldwide use these technologies to improve efficiency, transparency, and accountability. This has changed the fundamental relationship between citizens and the state by creating new possibilities for service delivery, financial inclusion, and participation in governance. However, concerns also remain about privacy, surveillance, accountability, and digital exclusion. Early scholarship focused on how ICT could improve public service delivery and administrative efficiency. Now the literature has expanded to include examination of broader implications of digital platforms, artificial intelligence and machine learning for governance and citizenship. Contemporary debates on digital state, platform governance, surveillance capitalism, and algorithmic governance highlight that better digital governance is not just the result of technological innovation. It is also shaped by institutional arrangements, and citizen trust. Unequal access to infrastructure, digital skills, and technological capabilities can deepen existing social and economic inequalities.

Much of the existing literature focuses on individual technologies or single-country experiences. As a result, relatively few comparative studies explain why the adoption of similar digital technologies produces different governance outcomes. This gap is addressed in this study by comparing Estonia, India and Kenya through the dimensions of state capacity, legitimacy and digital inclusion. These countries differ significantly in terms of population size, level of development, and administrative capacity. But all have adopted digital technologies as an important part of governance. Estonia is a highly developed digital state based on institutional trust and interoperable public services (Diaz, 2021). India represents a large-scale, state-led model of Digital Public Infrastructure. Kenya represents a more market-led model shaped by mobile technology and private sector innovation. By bringing together three contrasting models of digital transformation, the study contributes to comparative digital governance scholarship by demonstrating how differences in state capacity, legitimacy and digital inclusion shape divergent governance outcomes.

There are three interrelated research questions. First, how do state capacity, legitimacy and digital inclusion influence digital governance outcomes? Second, despite the adoption of similar digital technologies, why do these

countries experience different governance outcomes? Third, what lessons do these experiences offer for developing countries seeking to adopt digital technologies in governance? To address these questions, this study adopts a qualitative comparative case study approach based on secondary sources, including academic literature, policy reports, and publications from international organisations. The comparison is organised around three analytical dimensions – state capacity, legitimacy and digital inclusion – to provide a consistent framework for examining the three cases. State capacity is examined through the ability of public institutions to develop and regulate digital systems, legitimacy through public trust, transparency, and accountability, and digital inclusion through access to digital infrastructure, affordability, and digital skills.

By comparing the experiences of Estonia, India and Kenya, the study argues that strong state capacity, public trust and inclusive governance are critical determinants of successful digital transformation. Where institutions are weak, regulatory safeguards are inadequate, or accountability mechanisms are ineffective, adoption of digital systems can reinforce existing inequalities, raise concerns about surveillance and weaken public confidence in government. The findings therefore suggest that technological innovation alone is insufficient to improve governance. Rather, effective digital governance depends on institutions that are capable, accountable and trusted, supported by governance systems that are inclusive, and responsive to citizens.

Contemporary Perspectives on Digital Governance: An Analytical Framework

Digital governance is not just about the use of digital technology in government administration. It has evolved much beyond. The adoption of tools like digital identity systems, artificial intelligence, and algorithmic decision-making has shifted the focus from technology to the institutional arrangements that shape its use. Recent studies show that the success of digital governance depends not on adopting technology alone, but equally on the quality of public institutions, regulatory frameworks, and citizens' trust (OECD, 2024; World Bank, 2024). Because of this, countries implementing similar technologies often experience very different governance outcomes depending on the political and institutional context in which they operate.

To explain these differences, the study draws on state capacity theory as its primary theoretical perspective. As Fukuyama (2004) points out, state capacity refers to the ability of governments to design, implement, and sustain

public policies effectively. In the context of digital governance, it includes building reliable digital public infrastructure, protecting personal data, regulating emerging technologies and ensuring that public institutions can respond effectively to technological change. However, state capacity alone cannot fully explain the differences in governance performance. They are also influenced by legitimacy and digital inclusion. Therefore, the study brings together these three dimensions in an analytical framework to examine how these interact to shape digital governance outcomes in Estonia, India and Kenya.

State Capacity

State capacity is an important determinant of the success of digital governance. In the digital era, this involves more than carrying out routine administrative functions. Governments must be able to develop secure digital infrastructure, protect personal data, regulate emerging digital technologies, strengthen cybersecurity, and deliver reliable digital public services. Countries with strong state capacity respond faster and more effectively to rapid technological changes and digital transformations. It helps build public trust and deliver digital services in an effective and equitable manner. In this study, state capacity serves as a foundation for explaining why digital governance outcomes differ across countries.

Legitimacy

Institutional capacity alone is not sufficient to ensure effective digital governance. Citizens must also trust the institutions and believe that they operate fairly, transparently and in the public interest. Legitimacy refers to the extent to which government institutions and actions are seen as trustworthy, accountable and responsive to citizens' needs. As Lipset (1959) argues, legitimacy is the key source of political stability because people are more willing to accept and comply with institutions they consider legitimate. In the context of digital governance, public trust grows when governments protect the privacy of citizens, ensure transparency in the use of digital technologies, and provide effective mechanisms for grievance redressal. Higher levels of public trust encourage wider use of digital public services and enhance digital inclusion.

Digital Inclusion

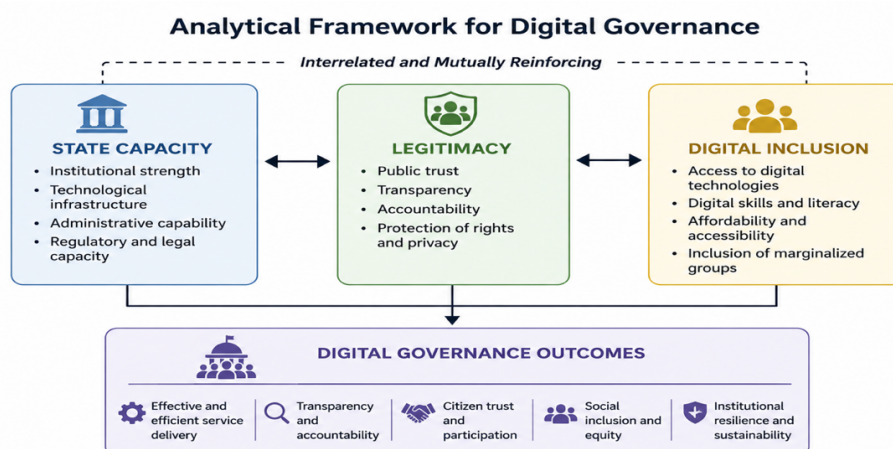
Digital inclusion refers to the extent to which people can access and effectively use digital services regardless of their income, age, gender, or

geographical location. It is not just about availability of digital infrastructures rather access to affordable internet, digital literacy, accessible technologies, and supportive public policies. If a section of society remain excluded from digital services, even well-designed digital systems can reinforce inequality. Therefore, digital inclusion is an important measure of digital transformation.

These three determinants are closely interconnected and reinforce one another. Governments with stronger state capacity are more capable of developing secure digital infrastructure, regulating modern technologies, and delivering reliable public services. When these institutions function transparently and accountably, they are more likely to gain public trust, strengthening the legitimacy of digital governance. Greater legitimacy leads to wider citizen participation and more inclusive digital systems.

The opposite is equally true. Weak state capacity can lead to weak implementation, inadequate regulatory oversight, and lower public confidence in digital institutions. Limited digital inclusion can reinforce existing inequalities and prevent many citizens from fully benefiting from digital public services. Digital governance should therefore be viewed not simply as a technological process but as an institutional one, where governance outcomes depend on the interaction between state capacity, legitimacy, and digital inclusion rather than on technology alone (Mazzucato & Kattel, 2020; OECD, 2024).

Figure 1: Analytical framework showing the relationship between state capacity, legitimacy, digital inclusion, and digital governance outcomes.



Source: Developed by the author.

Estonia: Digital Trust, State Capacity and Institutional Resilience

Through its remarkable digital transformation journey, Estonia has emerged as a model of innovative governance. Widely regarded as the world's most advanced digital society (Estonia, n.d.), Estonia has transformed governance by implementing cutting-edge digital technologies. After gaining independence in 1991, Estonia embarked on a digital transformation journey. Most of the existing infrastructure was Soviet-era legacy; less than half of the Estonian population even had a phone line (Harvard Ash Centre, 2017). Seeing this as an opportunity to build low-cost, cutting-edge systems based on accessibility and efficiency, the government pushed through a period of modernization, establishing the foundations of a digital age. The IT development strategy of 1994, the "Principles of Estonian Information Policy", which was approved in 1998, created a funding of 1% of GDP for IT development (e-Estonia, n.d.).

One of the main cornerstones of Estonia's digital transformation was the Tiger Leap programme initiated in 1996. It aimed at investing heavily in the development and expansion of computer and network infrastructure in Estonia through public private partnerships, with a particular emphasis on education. As a result, by 1997, 97% of Estonian schools had an internet connection (Northern Birch Credit Union, 2018). The next major developments in the Estonian digitalization journey were the establishment of the first e-banking services (1996) and e-cabinet (2000) for the government, the opportunity for Estonians to declare their taxes online through the e-tax authority since 2000 (e-Estonia, 2021).

One of the key pillars of Estonia's digital ecosystem is the X-Road interoperability platform, which enables secure data exchange between public agencies and private institutions. The main purpose of X-Road was to provide a secure platform for exchanging data while protecting sensitive information. Rather than creating one central database, it allows public agencies, private institutions, and businesses to share authorized data securely while retaining control over their own databases (Nordic Institute for Interoperability Solutions, n.d.). X-tee, which uses X-Road technology, has become the backbone of Estonia's digital state, allowing public and private information systems to work together securely. Ninety nine percent of public services are accessible online 24/7 (e-Estonia, 2021).

The development of digital identity systems, electronic taxation, e-health services, online business registration, and internet voting has together created a highly integrated digital governance system (World Bank, 2023). There is a high

level of coordination among government agencies, supported by interoperable digital infrastructure and a clear legal framework for data sharing. This has enabled public institutions to deliver integrated services while reducing duplication and improving administrative efficiency. Estonia has also developed robust legal frameworks, cybersecurity institutions, and the administrative capacity to manage increasingly complex digital infrastructures. These institutional arrangements have strengthened the state's capacity to manage digital governance effectively.

Legitimacy is reinforced through transparency and accountability mechanisms that allow citizens to monitor who accesses their personal information. In 2002, Estonia created a digital identification system, based on the mandatory ID card. The e-Identity system means that all Estonian nationals and residents, regardless of location, have a state-issued electronic identity, called e-ID which enables them to interact with the state and use a wide range of its services. People use their e-IDs to pay bills, vote online, sign contracts, shop, access their health information, and much more (e-Estonia, n.d.). Using their e-ID to log in to the state portal, citizens can use the Data Tracker to view records of operations performed on their personal data (Estonian Information System Authority, 2026). Thus, by giving citizens visibility over access to their personal data, this digital system strengthens trust in public institutions. This transparency creates accountability, as government officials know that improper access can be detected. At the same time, secure and convenient digital services demonstrate the state's capacity to meet citizens' everyday needs, reinforcing the legitimacy of digital governance.

The 2007 cyberattacks marked a turning point in Estonia's digital development. Coordinated attacks on government institutions, banks, and media organisations exposed vulnerabilities in the country's digital infrastructure (European Union Committee, 2010). These attacks served as a wake-up call for Estonia, highlighting the need for stronger cybersecurity measures. Following the attacks, Estonia strengthened its national cybersecurity policies. It also improved cooperation between public and private institutions and supported the establishment of the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn (North Atlantic Treaty Organization, 2007). Estonia's digital ecosystem has also been aligned with European Union regulatory frameworks, particularly the General Data Protection Regulation (GDPR), which strengthens safeguards for personal data and privacy. Together, these cybersecurity measures and legal protections have further strengthened citizen trust and democratic accountability.

Estonia's emphasis on digital sovereignty extends beyond cybersecurity. Estonia maintains state control by placing key systems under the oversight of public authorities. For example, the Estonian Information System Authority (RIA), a government agency, administers the national e-ID infrastructure, the X-tee data-exchange layer, and national cybersecurity coordination (Estonian Information System Authority, n.d.). Government agencies also retain control of their own databases, while X-Road enables secure and regulated data sharing rather than placing all information in one central database. Estonia additionally backs up critical state data through its Data Embassy, whose resources remain under Estonian state control even though they are physically located abroad (e-Residency of Estonia, n.d.).

Although internet penetration and digital literacy are among the highest in the world, some groups remain excluded. Older adults, rural communities, and Russian-speaking minorities still face difficulties related to digital skills, language accessibility, and unequal access to digital resources (World Bank, 2024; United Nations, 2024). Recognizing these challenges, the Estonian government has invested in digital literacy programmes and inclusive service delivery initiatives to reduce digital exclusion.

The Information System Authority (RIA) has offered free digital-safety workshops for middle-aged and older adults in libraries across the country, helping participants build confidence in using the internet and protecting personal data (Estonian Information System Authority, 2025). To improve rural connectivity, the government has supported the EstWin broadband project and later "last-mile" funding measures to extend high-speed internet infrastructure to sparsely populated areas (Ministry of Justice and Digital Affairs, n.d.). In addition, the *Let's Learn Together* programme provides multilingual support, including Russian-language resources, to help families engage with Estonia's education system (Education and Youth Board, n.d.).

The Estonian experience suggests that digital governance is more effective when technological innovation is supported by strong state capacity, legitimacy and inclusive governance. Beyond adoption of advanced technologies, the ability of Estonia's public institutions to establish interoperable digital infrastructure, robust cybersecurity, clear legal safeguards and transparency mechanisms have led to its success. Higher levels of public trust have, in turn, reinforced citizen participation and enabled widespread adoption of digital public services. Estonia therefore illustrates how state capacity,

legitimacy, and digital inclusion can operate in a mutually reinforcing manner to produce resilient and sustainable digital governance.

India: Scale, Efficiency and Digital Governance

India has embarked on a vision to transform into a digitally empowered society and knowledge economy. Due to its massive population, India's digital transformation has been driven by the challenge of governing at scale. Through Aadhaar, the Jan Dhan–Aadhaar–Mobile (JAM) architecture, and the broader Digital Public Infrastructure (DPI), the government has sought to improve service delivery, expand financial inclusion, and enhance administrative efficiency (World Bank, 2024; OECD, 2024).

Aadhaar has emerged as a cornerstone of India's digital transformation and has evolved into the world's largest biometric identity programme. The large-scale identification programme was initiated with the establishment of the Unique Identification Authority of India (UIDAI) on 28 January 2009 through a notification of the Planning Commission (now NITI Aayog). Later, the programme was formally named “Aadhaar”. According to the Unique Identification Authority of India (UIDAI) Aadhaar Dashboard, more than 1.44 billion Aadhaar numbers have been generated as of July 2026 (UIDAI, 2026).

Aadhaar is widely used for a variety of public services and administrative purposes. The Aadhaar project has been integrated with several welfare and social security programmes, including the domestic LPG subsidy scheme and the Mahatma Gandhi National Rural Employment Guarantee Act (MGNREGA) (UIDAI, 2026). Under these Direct Benefit Transfer (DBT) schemes, the subsidy money is directly transferred to Aadhaar-linked bank accounts. In July 2014, Aadhaar-enabled biometric attendance systems were introduced in government offices. The system was introduced to check late arrivals and absenteeism among government employees (Government of India, 2014). In addition, Aadhaar has been utilized for various other purposes, including passport issuance (Ministry of External Affairs, 2016), income tax filing (Government of India, 2017), and linking Employees' Provident Fund (EPF) accounts (EPFO, 2021).

Together with the Jan Dhan financial inclusion programme and expanding mobile connectivity, it forms the foundation of India's Digital Public Infrastructure. Platforms such as CoWIN, DigiLocker, the Unified Payments Interface (UPI), and Direct Benefit Transfer (DBT) have transformed the delivery of public services by improving administrative coordination, reducing leakages, and facilitating faster access to welfare benefits (Srinivasan, 2025).

From the perspective of state capacity, these initiatives represent important achievements in India's digital governance architecture. By integrating digital identity, banking, and payment systems, the government has strengthened its capacity to identify beneficiaries, coordinate service delivery, and implement welfare programmes. During the COVID-19 pandemic, digital platforms such as CoWIN facilitated large-scale vaccine registration, while the DBT system facilitated the transfer of financial assistance to millions of beneficiaries (Government of India, 2023; UIDAI, 2024).

While India's state capacity expanded rapidly through digital governance initiatives, there are concerns over legitimacy. The institutional mechanisms responsible for governing the digital ecosystem have not developed at the same pace. This imbalance raises important questions about transparency, accountability and public trust in digital governance. For instance, while supporters view Aadhaar as an important instrument for reducing corruption, eliminating duplicate beneficiaries, and improving service delivery, critics argue that the large-scale collection of biometric and demographic data raises concerns about privacy, surveillance, and the concentration of state power.

These debates gained constitutional significance with the Supreme Court's landmark decision in *Justice K. S. Puttaswamy (Retd.) v. Union of India* (2017), in which privacy was recognized as a fundamental right. In its subsequent Aadhaar judgment, *Justice K. S. Puttaswamy (Aadhaar-5J.) v. Union of India* (2018), the Court upheld the constitutional validity of Aadhaar but limited its mandatory use, particularly by private entities. These judgments established important constitutional principles relating to proportionality, necessity, and informational privacy, placing legal limits on the expansion of digital governance.

Another important step in strengthening India's data governance framework is the enactment of the Digital Personal Data Protection Act, 2023. The legislation establishes a consent-based approach to data processing and sets out obligations for the collection, use and storage of personal information. However, broad exemptions for government agencies raise concerns about the effectiveness of regulatory oversight and the independence of the enforcement mechanism (Joint Committee on the Personal Data Protection Bill, 2021; PRS Legislative Research, 2023).

Ultimately, the legitimacy of digital governance depends not only on administrative efficiency but also on citizens' confidence that digital systems operate fairly, transparently, and with adequate protection for individual rights.

Persistent concerns regarding surveillance and limited accountability erode the legitimacy of the digital governance infrastructure. Digital inclusion also remains uneven because of disparities in internet connectivity, digital literacy, language accessibility, and broader socio-economic conditions. Older adults, tribal communities, migrant workers, persons with disabilities, and other vulnerable groups often encounter difficulties in accessing and using digital services (Medianama, 2024). Aadhaar-based authentication failures have become one of the most widely debated challenges within India's digital governance system. Biometric mismatches, unreliable internet connectivity, and technical errors have occasionally prevented beneficiaries from receiving food rations, pensions, and other welfare benefits (UNDP, 2024; Saxena, 2017). In addition, grievance redressal mechanisms remain fragmented and are often difficult for marginalized communities to access. Beneficiaries affected by technological failures often face obstacles to challenging automated decisions or correcting inaccurate records. As a result, improvements in administrative efficiency do not always translate into equitable access or democratic accountability.

Thus, India's experience demonstrates that Digital Public Infrastructure can significantly expand state capacity by enabling large-scale service delivery, financial inclusion, and administrative coordination. However, the rapid expansion of DPI has not always been accompanied by corresponding improvements in regulatory oversight, accountability, and citizen trust. As a result, concerns over privacy, surveillance, data protection, and digital exclusion continue to shape the legitimacy of India's digital governance model. Therefore, the Indian case suggests that improvements in administrative efficiency alone are insufficient to ensure effective digital governance unless they are supported by robust institutions, regulatory safeguards, and inclusive access to digital services.

Kenya: Platform Governance, Digital Innovation and Regulatory Challenges

Kenya's digital transformation has evolved primarily through market-led initiatives. Much of this transformation has been shaped by the success of M-Pesa, launched by Safaricom in 2007 (Mas & Radcliffe, 2010). Originally developed as a mobile money transfer service, M-Pesa has evolved into a broader digital financial ecosystem supporting payments, remittances, savings, credit, and microfinance. The platform has also facilitated innovative services such as M-KOPA, which offers pay-as-you-go solar energy financing, and M-TIBA, a mobile-based healthcare platform. Alongside these developments, the Kenyan

government has expanded the eCitizen portal, bringing together services related to taxation, identity documents, licensing, and land administration (World Bank, 2019).

Unlike Estonia and India, Kenya's digital infrastructure is shaped largely by private-sector actors rather than state institutions. As a result, the state's digital capacity has often depended on partnerships with dominant technology companies. In Kenya, Safaricom occupies a particularly influential position, accounting for more than 60 per cent of the mobile telecommunications market while M-Pesa remains the dominant mobile money platform in the country (Safaricom, 2024). Its dominant role has effectively made the company a quasi-public provider of essential digital infrastructure. Although this concentration has accelerated innovation and expanded service delivery, it has also increased dependence on a single private platform and raised important questions about competition, accountability, democratic oversight, and the balance between public authority and corporate power (OECD, 2024).

In order to improve legitimacy and public trust the Kenyan government enacted Data Protection Act (2019) and established the Office of the Data Protection Commissioner (ODPC) (Government of Kenya, 2019; ODPC, 2024). These measures marked important steps towards strengthening privacy protection and safeguarding digital rights. Kenya's digital transformation also aligns with broader continental efforts under the African Union's Digital Transformation Strategy (2020–2030), which seeks to strengthen digital infrastructure, digital rights, and regional cooperation (African Union, 2020). However, regulatory institutions continue to face resource constraints, while public awareness of data protection remains relatively limited (ODPC, 2024). There are also concerns about transparency, consent, and the misuse of personal information. (Digital Watch Observatory, 2024).

One of Kenya's greatest achievements has been the expansion of financial inclusion. Mobile money services have enabled millions of previously unbanked citizens to participate in the formal economy and access financial services. Women, rural communities, and low-income households have particularly benefited from mobile-based payments and microfinance services. However, regional disparities in internet access, affordability, and digital literacy continue to limit participation in digital governance. Many vulnerable groups still face barriers to reliable connectivity and the effective use of increasingly complex digital platforms (United Nations, 2024).

Kenya's experience shows that even where state capacity is comparatively limited, private-sector innovation can drive rapid digital transformation. Market-led platforms such as M-Pesa have expanded financial inclusion and improved access to digital services. At the same time, reliance on dominant technology companies has created new governance challenges relating to regulatory oversight, platform dependence, competition, and accountability. Therefore, while market-led innovation can compensate for limited state capacity, the Kenyan example suggests that long-term legitimacy and sustainability depend on the ability of public institutions to regulate digital ecosystems effectively and safeguard citizens' rights.

Comparative Analysis: Institutions, Legitimacy and Divergent Pathways of Digital Governance

The experiences of Estonia, India, and Kenya reveal how similar technologies can lead to very different governance outcomes depending on political will, institutional strength, and social context. Each represents a distinct model of digital transformation: Estonia- an institution-led model, India- a state-led Digital Public Infrastructure model, and Kenya - a market-led platform model. Table 1 provides a comparative overview of the three cases.

Table 1. Comparative Overview of the Three Cases

Dimension	Estonia	India	Kenya
Governance Model	Trust-based digital state	State-led Digital Public Infrastructure	Market-led digital ecosystem
Primary Driver	Institutional modernization	Population-scale service delivery and welfare	Private-sector innovation and mobile technologies
State Capacity	Strong institutional and regulatory capacity	High implementation capacity with uneven regulatory oversight	Moderate capacity relying on public-private partnerships
Legitimacy	High public trust supported by transparency, legal safeguards,	Mixed; efficiency gains alongside concerns over	Mixed; convenience and financial inclusion alongside concerns

	and cyber resilience	privacy and surveillance	over corporate dominance
Digital Inclusion	High; broad access with targeted support for vulnerable groups	Expanded access but uneven due to digital and socio-economic disparities	Improved financial inclusion but gaps remain in connectivity, affordability, and digital literacy
Key Governance Challenge	Maintaining cyber resilience and inclusive access	Balancing efficiency with privacy, accountability, and inclusion	Strengthening regulation and reducing platform dependency
Overall Outcome	Resilient and trusted digital governance	Scalable but contested digital governance	Innovative but regulation-dependent digital governance

Source: *Compiled by the author based on the comparative analysis.*

State Capacity and Digital Governance

State capacity directly explains these differences in outcomes. Estonia's success reflects sustained investment in digital infrastructure, interoperability, and administrative reform, which enabled the development of an integrated digital state. India followed a different trajectory by using Digital Public Infrastructure and strong executive coordination. It helped expand digital services at an unprecedented scale, although challenges relating to grievance redressal and data protection continue to limit institutional effectiveness. In Kenya, digital transformation has been driven largely by private-sector innovation, with platforms such as M-Pesa compensating for relatively limited state capacity.

Legitimacy and Public Trust

Public trust influences how citizens respond to digital governance initiatives. In Estonia, transparency, strong cybersecurity, and citizens' ability to monitor access to their personal data have reinforced confidence in digital institutions. In India, while Aadhaar and Digital Public Infrastructure have improved service delivery, continuing debates over privacy, surveillance, and exclusion have led to concerns over digital governance. Kenya reflects another pattern. Citizens have widely adopted mobile platforms because of their

convenience and accessibility but questions around platform dependence and regulatory oversight continue to influence trust in the digital ecosystem.

Digital Inclusion

Although all three countries have expanded digital services, the question of expansion of digital inclusion differs considerably. In Estonia, the main challenges relate to older citizens and linguistic minorities who may still face barriers to full participation in digital services. In India, digital inclusion is shaped by wider socio-economic inequalities, with biometric authentication failures, limited digital literacy, and unequal access continuing to affect vulnerable groups. Kenya's experience highlights a different set of challenges, particularly those associated with affordability, smartphone ownership, and dependence on mobile network operators.

Key Lessons

The experiences of Estonia, India, and Kenya illustrate that there is no single pathway to successful digital governance. Although all three countries have embraced digital technologies to improve governance, they have done so under different institutional, political, and socio-economic conditions. As a result, each has followed a distinct trajectory of digital transformation, producing different opportunities as well as different governance challenges.

A common lesson emerging from the three cases is that technology, by itself, cannot guarantee better governance. Its effectiveness depends on governments having the institutional capacity to regulate digital ecosystems, protect citizens' rights, and build public trust. Equally important is ensuring that digital services remain accessible to all sections of society. Where these conditions are absent, digital transformation may reinforce existing inequalities and create new concerns relating to exclusion, privacy, and accountability (OECD, 2024; United Nations, 2024).

The comparison also highlights the close relationship between state capacity, legitimacy, and digital inclusion. Strong state institutions provide the foundation for effective regulation and reliable digital services, while transparent and accountable governance strengthens public confidence in digital systems. Greater public trust, in turn, encourages wider participation and helps extend the benefits of digital transformation. This interaction explains why countries adopting similar digital technologies often experience different governance outcomes (Ariyadi & Akbar, 2025).

Taken together, these findings suggest that digital governance should be understood primarily as an institutional and political process rather than a technological one. Technology undoubtedly expands the possibilities for improving governance, but its long-term impact depends on capable institutions, effective regulation, public trust, and inclusive policies that ensure the benefits of digital transformation are shared across society.

Conclusion

Digital transformation has become a defining feature of contemporary governance, changing the ways in which governments deliver public services and engage with citizens. Through a comparative analysis of Estonia, India, and Kenya, the study shows that digital governance is shaped not simply by technological innovation but by the institutional environments within which digital technologies are adopted and governed. The findings demonstrate that state capacity, legitimacy, and digital inclusion are closely interconnected and together influence whether digital transformation strengthens governance or creates new forms of inequality, exclusion, and regulatory challenge.

Beyond its empirical findings, this study contributes to the comparative digital governance literature by arguing that digital technologies on their own cannot explain digital governance effectiveness. Instead, differences in state capacity shape public legitimacy and digital inclusion, which together influence governance outcomes. By comparing three contrasting pathways of digital transformation, the study develops an analytical framework that explains why similar digital technologies produce different outcomes under different institutional conditions. In doing so, it moves beyond technology-centered explanations of digital transformation and highlights the importance of state capacity, legitimacy, and digital inclusion in shaping digital governance. The study therefore offers an institutional explanation for divergent pathways of digital governance across different political and developmental contexts. The proposed analytical framework may also be applied to comparative studies beyond the three cases examined here.

The findings also have important implications for policymakers. Governments seeking to expand digital governance should view technology not as an end in itself but as part of a broader programme of institutional reform. Investments in digital infrastructure need to be accompanied by effective regulatory frameworks, strong accountability mechanisms, robust data protection, and sustained efforts to promote digital inclusion. As artificial

intelligence becomes increasingly integrated into public administration, ensuring transparency, explainability, and meaningful human oversight will be essential for maintaining democratic legitimacy and public confidence.

The comparative analysis further suggests that there is no universal model of digital governance. Estonia, India, and Kenya illustrate that digital transformation follows different institutional pathways shaped by national priorities, governance capacities, and social conditions. Rather than replicating successful models from elsewhere, governments should adapt digital reforms to their own institutional realities while strengthening the capacities needed to regulate emerging technologies and protect citizens' rights.

Ultimately, the success of digital governance should not be measured solely by the sophistication of technology or the speed of service delivery. Its long-term effectiveness depends on institutions that are capable, accountable, and trusted, and on governance systems that ensure the benefits of digital transformation are shared broadly across society. Technology can expand the possibilities of governance, but it is the quality of institutions that ultimately determines whether digital transformation contributes to more democratic, inclusive, and sustainable forms of governance.

References

- African Union. (2020). *Digital Transformation Strategy for Africa (2020–2030)*. African Union.
- Ariyadi, A., & Akbar, M. (2025). Public services in the digital age: A systematic review and bibliometric analysis of trends and challenges in digital governance. *Journal of Government and Development*, 2(2), 153–167. <https://doi.org/10.69816/jgd.v2i2.46068>
- Bratton, B. H. (2016). *The stack: On software and sovereignty*. MIT Press.
- Desai, A., & Manoharan, A. P. (2024). Digital transformation and public administration: The impacts of India's Digital Public Infrastructure. *International Journal of Public Administration*, 47(9), 575–578. <https://doi.org/10.1080/01900692.2024.2350762>
- Diaz, J. (2021). *Towards more 'e-volved' democracy: An exploration of digital governance in Estonia and the lessons it holds for strengthening democracy in the United States* (NEXTEUK Working Paper Series). <https://doi.org/10.2139/ssrn.3999376>
- Digital Watch Observatory. (2024). *Kenya data protection*. <https://dig.watch>

- e-Estonia. (2021, October 20). *X-Road*. <https://web.archive.org/web/20221016104559/https://e-estonia.com/solutions/interoperability-services/x-road/>
- e-Estonia. (2024a). *Data transparency and citizen control*. <https://e-estonia.com>
- e-Estonia. (n.d.). *ID-card*. <https://web.archive.org/web/20210326221335/https://e-estonia.com/solutions/e-identity/id-card/>
- e-Estonia. (n.d.). *Story: The world's most advanced digital society*. <https://e-estonia.com/story/>
- Education and Youth Board. (n.d.). *Let's learn together*. <https://harno.ee/en/lets-learn-together>
- Employees' Provident Fund Organisation. (2021). *Aadhaar seeding with Universal Account Number (UAN)*. Government of India.
- Estonia. (n.d.). *Overview: Welcome to the world's most digitally advanced society*. Retrieved August 4, 2026, from <https://estonia.ee/overview>
- Estonian Information System Authority. (2025, September 8). *RIA organises cybersecurity workshops for middle-aged and older adults*. <https://ria.ee/uudised/ria-korraldab-kuberturvalisuse-opitubasid-kesk-ja-vanemaealiste>
- Estonian Information System Authority. (2026, April 30). *Data tracker*. <https://ria.ee/en/state-information-system/people-centred-data-exchange/data-tracker>
- Estonian Information System Authority. (n.d.). *eID ecosystem governance*. <https://www.ria.ee/en/state-information-system/electronic-identity-eid-and-trust-services/eid-ecosystem-governance>
- European Commission. (2024). *General Data Protection Regulation (GDPR)*. <https://commission.europa.eu>
- European Union Committee. (2010). *Protecting Europe against large-scale cyber-attacks* (HL Paper 68). UK Parliament. <https://publications.parliament.uk/pa/ld200910/ldselect/ldeucom/68/6805.htm>
- Fukuyama, F. (2004). *State-building: Governance and world order in the 21st century*. Cornell University Press.
- Government of India. (2014). *Implementation of Aadhaar Enabled Biometric Attendance System*. Department of Electronics and Information Technology.

- Government of India. (2017). *Finance Act, 2017* (Section 139AA of the Income-tax Act, 1961).
- Government of India. (2023). *Lok Sabha Unstarred Question No. 1686: Digital public infrastructure*. <https://sansad.in/getFile/loksabhaquestions/annex/1714/AU1686.pdf?source=pqals>
- Government of Kenya. (2019). *Data Protection Act, No. 24 of 2019*.
- Gorwa, R. (2019). What is platform governance? *Information, Communication & Society*, 22(6), 854–871. <https://doi.org/10.1080/1369118X.2019.1573914>
- Harvard Ash Center. (2017, May 15). *E-stonia: One small country's digital government is having a big impact*. Medium. <https://medium.com/innovations-in-government/e-stonia-one-small-countrys-digital-government-is-having-a-big-impact-a33e30983c0b>
- Joint Committee on the Personal Data Protection Bill, 2019. (2021). *Report of the Joint Committee on the Personal Data Protection Bill, 2019*. Rajya Sabha Secretariat.
- Justice K. S. Puttaswamy (Aadhaar-5J.) v. Union of India*, (2019) 1 SCC 1.
- Justice K. S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors.*, (2017) 10 SCC 1.
- Lee, J., & Dai, Y. (2025). Artificial intelligence and data-driven technology in the public policy cycle: Comparative applications, opportunities, and risks. *Journal of Comparative Policy Analysis: Research and Practice*, 27(5–6), 477–493. <https://doi.org/10.1080/13876988.2025.2598371>
- Lipset, S. M. (1959). Some social requisites of democracy: Economic development and political legitimacy. *American Political Science Review*, 53(1), 69–105. <https://doi.org/10.2307/1951731>
- Mas, I., & Radcliffe, D. (2010). *Mobile payments go viral: M-PESA in Kenya*. World Bank. <https://documents.worldbank.org/en/publication/documents-reports/documentdetail/638851468048259219>
- Mazzucato, M., & Kattel, R. (2020). *COVID-19 and public-sector capacity* (IIPP Working Paper WP 2020-12). UCL Institute for Innovation and Public Purpose.

- Medianama. (2024, March 7). *India's Digital Personal Data Protection Act: Challenges and implications for digital governance*. <https://www.medianama.com/>
- Ministry of Electronics and Information Technology. (2024). *Digital India annual report 2023–24*. Government of India. <https://www.meity.gov.in>
- Ministry of External Affairs. (2016). *Passport Seva: Aadhaar as proof of identity and address*.
- Ministry of Justice and Digital Affairs. (n.d.). *Broadband network construction support measures*. <https://www.justdigi.ee/digi-side-jakuber/uhenduvus/lairibavorkude-rajamise-toetusmeetmed>
- Nordic Institute for Interoperability Solutions. (n.d.). *X-Road history*. <https://web.archive.org/web/20221016124304/https://x-road.global/xroad-history>
- North Atlantic Treaty Organization. (2007, June 14). *NATO to strengthen protection against cyber attacks*. <https://www.nato.int/en/news-and-events/articles/news/2007/06/14/nato-to-strengthen-protection-against-cyber-attacks>
- Northern Birch Credit Union. (2018, February 16). *From no landlines to one of the most advanced e-societies in the world: Tech in Estonia*. <https://web.archive.org/web/20221016104557/https://blog.northernbirchcu.com/2018/02/16/from-no-landlines-to-one-of-the-most-advanced-e-societies-in-the-world-tech-in-estonia/>
- Office of the Data Protection Commissioner. (2024). *Data Protection Handbook*.
- Organisation for Economic Co-operation and Development. (2024). *Digital government index 2024: Results and key findings*. OECD Publishing. <https://doi.org/10.1787/1a89ed5e-en>
- PRS Legislative Research. (2023). *The Digital Personal Data Protection Bill, 2023*. <https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023>
- Safaricom PLC. (2024). *Annual report and financial statements 2024*.
- Saxena, N. C. (2017). *Issues in the implementation of Aadhaar and its implications for welfare delivery*. Centre for Equity Studies.
- Srinivasan, R. (2025). *State of DPI in India 2025*. Centre for Digital Public Goods, Indian Institute of Management Bangalore & Protean eGov Technologies.

- Taylor, L. (2017). What is data justice? The case for connecting digital rights and freedoms globally. *Big Data & Society*, 4(2), 1–14. <https://doi.org/10.1177/2053951717736335>
- UNESCO. (2021). *Recommendation on the ethics of artificial intelligence*.
- Unique Identification Authority of India. (2024). *Annual report 2023–24*. Government of India. https://uidai.gov.in/images/2023-24_Final_English_Final.pdf
- Unique Identification Authority of India. (2026). *Aadhaar dashboard*. Retrieved July 15, 2026, from https://uidai.gov.in/aadhaar_dashboard/
- United Nations. (2024). *United Nations e-government survey 2024: Accelerating digital transformation for sustainable development*. United Nations.
- United Nations Development Programme. (2024). *Human development report 2023/2024: Breaking the gridlock*. UNDP.
- Van Dijck, J., Poell, T., & de Waal, M. (2018). *The platform society: Public values in a connective world*. Oxford University Press.
- World Bank. (2019). *Kenya economic update: Accelerating Kenya's digital economy*. World Bank. <https://www.worldbank.org/en/country/kenya/publication/kenya-economic-update-accelerating-kenyas-digital-economy>
- World Bank. (2023). *GovTech case studies: Estonia*. World Bank.
- World Bank. (2024). *GovTech maturity index 2024: Advancing digital transformation in the public sector*. World Bank.
- Yeung, K. (2018). Algorithmic regulation: A critical interrogation. *Regulation & Governance*, 12(4), 505–523. <https://doi.org/10.1111/rego.12158>
- Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.