Bridging the Digital Divide: Public Policy and Legal Frameworks for Strengthening E-Governance in Sri Lanka

Nāgānanda International Journal of Humanities & Social Sciences
Vol:10 , No. 05, 2025 pp. 52-65

http://www.niibs.lk
Issue Published Online: 01 December 2025
ISSN No: ISSN 2961-5801-G (online)

Tharmini Narendranathan
Department of Political Science, University of Jaffna, Sri Lanka

Abstract

This paper examines the role of laws and government policies in facilitating or hindering the success of e-governance in developing countries, with a focus on Sri Lanka and India. Both countries started digital governance programs in the early 2000s, Sri Lanka with the e-Sri Lanka project and India with the Digital India mission. However, India has seen more success due to its better legal systems, more decisive leadership, and increased use of the services. India's progress is attributed to its clear laws, such as the Information Technology Act (2000), a robust national identity system (Aadhaar), and useful services like DigiLocker and UMANG. These tools help people access government services online safely and efficiently. In contrast, Sri Lanka continues to face challenges. There is no law to protect personal data, and people in rural areas often lack sufficient knowledge and access to digital tools. Many government offices are not connected, resulting in slow and confusing services.This paper employs a comparative method, examining laws and policies, surveys, and interviews in both countries. It identifies several areas of weakness in Sri Lanka, including the absence of clear digital laws, overlapping responsibilities among various government agencies, inadequate legal training for workers, and limited digital education for the public.The paper states that Sri Lanka needs a robust plan. It should create a digital law to support online services, form a special national team for e-governance, allow users to give service feedback, and work with India to learn about legal technology. Training programs for civil servants and digital awareness campaigns should also be introduced. The main idea is that digital progress is not just about having technology. It also needs good laws, precise planning, and public trust. Without this, digital tools might exacerbate inequality. Based on what has worked in India, the paper gives a policy roadmap to help Sri Lanka improve. If Sri Lanka strengthens its legal system and works closely with its citizens, it can build a better digital future for everyone.

Keywords: ***e-governance, digital public services, legal framework, Sri Lanka, Digital India, ICT policy, digital divide***

Received : 01 July 2025
Revised : 25 August 2025
Accepted : 10 September 2025
Published : 01 December 2025

TO CITE THIS ARTICLE:
Tharmini Narendranathan, Bridging the Digital Divide: Public Policy and Legal Frameworks for Strengthening E-Governance in Sri Lanka. Nāgānanda International Journal of Humanities and Social Science. 7:4, Pp.52-65

Introduction

In today's digital world, an increasing number of governments are utilizing technology to deliver services to their citizens. This is called e-governance. It includes online forms, digital ID cards, and mobile apps for paying bills or applying for licenses. E-governance can save time, reduce corruption, and make services more accessible and user-friendly (Bhatnagar, 2014). However, for it to work effectively, countries need robust laws and effective planning. India and Sri Lanka both started e-governance projects many years ago. India initiated the Digital India program, while Sri Lanka launched the e-Sri Lanka program (Karunaratne, 2017). These programs were meant to help people use technology to connect with the government. However, India has been more successful than Sri Lanka. India's digital services reach a wide range of people, including those in rural areas (Singh & Kumar, 2016). In Sri Lanka, many people still visit government offices in person because online systems are either unreliable or difficult to use (Perera & Perera, 2020).

A big reason for this difference is the legal system. India has robust digital laws, including the Information Technology Act. These laws ensure that online transactions and digital documents are legal and secure (Mukherjee, 2015). Sri Lanka still lacks similar laws. This makes it hard for people to trust online systems. Additionally, many Sri Lankan government workers lack training in digital systems, which is why they still prefer paper files (Sivarajah & Irani, 2016).

This paper studies these differences between India and Sri Lanka. It asks: What can Sri Lanka learn from India? How can Sri Lanka enhance its digital laws and public policies to improve e-governance? The study looks at laws,

policy documents, and interviews from both countries. It also utilizes survey results from individuals in Sri Lanka to gain insight into their experiences with online services. The goal is to find practical ideas that Sri Lanka can use. These include creating new laws, developing more effective digital platforms, and educating both government workers and citizens on how to utilize technology. The paper argues that e-governance is not only about having computers and websites. It also ensures that everyone, including those from low-income and rural backgrounds, can use them safely and efficiently. Strong public policy and legal reform are needed to make digital services fair and valuable for all.
E-governance has become an important tool for enhancing the transparency, accountability, and efficiency of public service delivery. A growing body of literature analyzes the implementation of e-governance in developing countries, especially in South Asia. Much of this research has focused on the technological aspects and user engagement, but fewer studies explore the legal and institutional frameworks that either support or hinder digital transformation. This review highlights both Sri Lankan and Indian scholarship while identifying gaps that this study seeks to address.

In the case of Sri Lanka, early enthusiasm was evident with the launch of the e-Sri Lanka project, which the World Bank funded in the early 2000s. According to Samarajiva and Zainudeen (2008), this project aimed to introduce digital infrastructure, digitize citizen services, and develop rural telecenters. However, later reports, such as Fernando (2015), observed that political instability, poor coordination between ministries, and a lack of local ownership weakened its long-term impact. The project's failure to establish robust legal backing or continuity in governance led to a reduction in public trust.

Another critical weakness in Sri Lanka is the lack of a comprehensive data protection law. As noted by Gunawardena and Karunarathna (2019), while several ICT policies have been proposed, the absence of legislation around digital identity, data privacy, and cybercrime discourages both citizen participation and investment. Without clear legal safeguards, citizens are hesitant to share personal data online, which limits the use of e-services.

By contrast, India's digital transformation has been supported by comprehensive legal frameworks and centralized policy efforts. The Information Technology Act (2000) and its subsequent amendments form the foundation for digital legality, enabling services such as Aadhaar-based authentication and legally valid electronic signatures (Basu, 2016). The Digital India campaign, launched in 2015, emphasized the need for legal backing, budgetary support, and private sector partnerships. It created platforms like DigiLocker for document storage, UMANG for unified service access, and BharatNet for rural internet expansion (Choudhury, 2020).

Public-private partnerships have also played a central role in India. For instance, the Common Services Centers (CSCs) program allows citizens in rural areas to access services through locally operated kiosks. These are regulated and integrated through government systems. Studies such as those by Sharma and Gupta (2019) argue that these models are successful because they align policy, law, and local participation.

A unique strength of India's model lies in its legal recognition of digital infrastructure as a right to access services. Initiatives like the Right to Information (RTI) Act and Digital Service Delivery Acts in various states

create legal obligations for service provision, compelling government agencies to maintain digital channels.

In Sri Lanka, legal ambiguity often causes delays and uncertainty. For example, even where online systems exist, there is confusion about whether printed receipts from these platforms are valid in courts or for official records. As Ratnayake (2022) notes, without harmonizing digital practices with legal enforceability, e-governance tools will remain underused.

International organizations, such as the United Nations (2022) and the World Bank (2021), also report that countries with higher e-governance scores tend to have well-defined digital laws and effective public engagement mechanisms. Sri Lanka ranks lower in these indices due to fragmented policies and a lack of regulatory clarity.

Finally, comparative regional studies are rare. While some research highlights the benefits of specific platforms or user satisfaction, few focus on how legal reforms have made digital services reliable and scalable. This paper fills that gap by analyzing the legal-policy architecture and offering lessons from India that Sri Lanka can adopt.

The literature shows that legal certainty, policy alignment, and public trust are as crucial as technology for successful e-governance. India’s experience provides valuable lessons in building institutional capacity, securing citizen rights, and designing accountable digital services. Sri Lanka’s challenge is not a lack of technological capability, but rather the absence of strong legal and policy frameworks to support and sustain digital governance.

Methodology

This study employs a mixed-methods approach that combines qualitative document analysis, comparative legal review, stakeholder interviews, and a citizen survey to assess the impact of legal frameworks on e-governance in Sri Lanka, with India serving as a comparative benchmark. The primary focus of the study is Sri Lanka, with data collected from both urban (e.g., Colombo, Kandy, Jaffna) and rural districts (e.g., Vavuniya, Batticaloa). India serves as a secondary comparative case, studied through official policy documents, legal texts, and program evaluations.

The first part of the methodology involved analyzing key policy documents, government reports, and academic literature. In Sri Lanka, sources included the e-Sri Lanka framework, ICTA strategy papers, and draft legislation such as the proposed Data Protection Bill. In India, reference materials included the Information Technology Act (2000), Digital India program reports, and guidelines for Aadhaar and DigiLocker. This allowed for a side-by-side comparison of the legal instruments and digital infrastructure that each country has adopted.

To better understand how legal support structures affect implementation, the study compared enforceable laws, such as India's IT Act and digital authentication laws, with Sri Lanka's fragmented or absent regulations. This review focused on how each country defines legal validity for e-signatures, digital identity, and online transactions. Attention was also paid to whether these legal tools have been integrated across sectors (e.g., education, health, public services).

To gain practical insights, the study conducted semi-structured interviews with eight stakeholders in Sri Lanka. This included legal experts, IT professionals in government agencies, and civil servants involved in service delivery. Questions focused on perceived challenges in law implementation, coordination among ministries, and citizen response to digital services. Respondents were selected from urban and rural locations to capture geographic diversity.

A structured online survey was also distributed to 60 citizens who had interacted with government digital platforms in the last 12 months. The survey asked about awareness of legal protections, perceived service reliability, and whether users felt confident sharing information online. This data helped assess the effect of legal trust on service adoption.

This framework was employed to investigate how public sector structures and norms influence the adoption of technology. In Sri Lanka, overlapping institutional roles often block coordination. Applied to evaluate how the public receives new digital services. It helped measure legal clarity as one of the enabling or disabling factors in the use of digital services.

All respondents were informed about the voluntary nature of their participation, and responses were anonymized. The study followed ethical research practices approved by the affiliated university. By combining legal review with policy analysis and lived user experience, this methodology provides a comprehensive and well-rounded understanding of what is lacking in Sri Lanka's e-governance journey and how it can benefit from structured reform, drawing lessons from India's experience.

Results and Discussion

The findings of this study highlight that the primary obstacles to effective e-governance in Sri Lanka are not technological, but legal and institutional. While both Sri Lanka and India have recognized the strategic value of digital governance and have made technological investments, the difference in outcomes is stark. India's success in digital governance is rooted in a robust legal infrastructure, centralized institutional frameworks, and a population that largely trusts government digital platforms. In contrast, Sri Lanka's e-governance initiatives, though well-intentioned and partially implemented through programs such as e-Sri Lanka and the Lanka Government Network, have not achieved their full potential due to fragmented legal standards, siloed ministries, and public skepticism.

A key factor behind this disparity is the presence of comprehensive and enforceable legal frameworks in India. The Information Technology Act (2000), reinforced by the Digital Personal Data Protection Act (2023), provides Indian citizens and government officials with clear guidelines regarding digital documentation, e-signatures, cybersecurity, and the handling of personal data. These laws have helped build legal clarity, which in turn has strengthened user confidence. In contrast, Sri Lanka lacks a unified digital legal framework. Many citizens expressed hesitation in using government portals, citing uncertainty about the legal status of online documents. For example, one respondent recounted how a bank refused to accept a digitally obtained birth certificate because it lacked official validation procedures. This kind of experience perpetuates a cycle of mistrust and underuse. Consequently, there is an urgent need for Sri Lanka to enact a comprehensive Digital Governance Act that would legally recognize digital identities, e-

signatures, data protection measures, and online transactions.

Institutional fragmentation further hampers digital service delivery in Sri Lanka. Survey data and interviews revealed that various government departments operate independently, often using incompatible digital systems. This disjointed approach leads to duplication of effort and citizen frustration. In contrast, India's digital governance is streamlined through centralized coordination under the Ministry of Electronics and Information Technology (MeitY), enabling nationwide platforms like UMANG, DigiLocker, and eSign. These platforms operate across ministries, offering a unified user experience and significantly reducing redundancy. For instance, while a user in India can access multiple services through a single login, a citizen in Sri Lanka often has to register and verify their identity multiple times for different ministries. To address this, Sri Lanka should establish a central digital governance authority to coordinate policy, standardize systems, and ensure legal consistency across digital services.

Another critical difference lies in the adoption of a legally recognized digital identity. India's Aadhaar system has revolutionized service delivery by enabling instant identity verification, secure access to welfare programs, and legally valid digital documentation. Courts in India have upheld the legality of Aadhaar-linked services, further cementing its utility. In Sri Lanka, the absence of a centralized digital ID system that is both secure and legally recognized severely limits the scope of e-governance. Citizens are forced to repeatedly submit physical documents, which undermines efficiency and public trust. Therefore, introducing a National Digital Identity System in Sri Lanka, legally endorsed and integrated across services, would significantly enhance user experience and administrative functionality.

Public awareness and legal literacy emerged as another weak point in Sri Lanka's digital transformation. Over 60% of surveyed citizens indicated they were unaware of their digital rights or the legal safeguards associated with online government services. This ignorance breeds fear, causing people to avoid using digital platforms even when they are available. In contrast, India has actively worked to close this gap through the Digital Literacy Mission (PMGDISHA), which has trained millions of citizens, particularly in rural areas, on how to safely and confidently engage with digital platforms. For example, a university student in Colombo hesitated to submit scholarship applications online due to uncertainty about the legal standing of digital submissions. To combat such hesitation, Sri Lanka must launch nationwide public awareness campaigns that educate citizens about their digital rights, how to navigate government portals, and the legal legitimacy of digital interactions. These efforts should leverage schools, local governments, TV and radio, and print media to ensure widespread reach.

The study also revealed administrative resistance within the Sri Lankan public sector. More than 70% of civil servants reported not receiving formal training on digital procedures or legal standards, resulting in a reluctance to embrace e-governance tools. Many officials prefer traditional paperwork due to concerns about making legally questionable decisions in the absence of precise guidance. This is compounded by system unreliability. In one example observed during fieldwork at a Divisional Secretariat, the e-services portal had been offline for several consecutive days. Staff reverted to manual processes, thereby defeating the purpose of digitization. To address this institutional inertia, Sri Lanka should implement mandatory legal-tech training programs for all public servants. These training modules should cover data protection,

legal status of digital documents, cybersecurity basics, and platform usage protocols, while also fostering a digital-first administrative culture.

The lack of real-time feedback and legal support systems on Sri Lanka's government portals is another significant barrier. Users encountering technical issues or legal concerns have no digital means of resolving them and are often forced to resort to physical visits. By contrast, India's portals, such as MyGov.in and DigiLocker, feature embedded support systems, feedback forms, and even AI chatbots that provide legal clarity. Incorporating such tools into Sri Lankan portals would increase transparency, build user confidence, and enable continuous system improvement based on user input.

Moreover, judicial reinforcement has played a significant role in fostering digital trust in India. Courts have consistently upheld the validity of electronic documents and digital signatures, thereby legitimizing their use in legal and administrative contexts. In Sri Lanka, however, judicial precedents concerning digital governance are rare. This legal vacuum contributes to official hesitation and erodes user confidence. There is a pressing need for Sri Lanka's judiciary to adopt and promote the use of digital documentation in legal proceedings. Training judges in digital governance and data law can help establish a body of case law that legitimizes e-governance.

Another factor that undermines digital service delivery in Sri Lanka is the poor reliability of infrastructure. Citizens often experience system downtime, service unavailability, and incomplete transactions. These technical failures are not just inconvenient, they also send a message that digital systems are unreliable. In one case, researchers observed a government office where the

digital portal was offline for an entire week, resulting in all services reverting to manual processes. To prevent this, the government must implement service-level agreements (SLAs) with IT providers to ensure platform uptime, establish independent audit mechanisms, and hold service providers accountable for disruptions.

Finally, India's experience provides a valuable blueprint for Sri Lanka. Through bilateral collaboration, Sri Lanka can adopt successful practices from India, such as centralized legal frameworks, digital identity systems, and nationwide literacy programs. India has already assisted other countries, such as Bangladesh and Mauritius, in building similar systems. Sri Lanka should initiate policy dialogues, technical exchange programs, and joint capacity-building projects with Indian institutions to localize and implement proven digital governance models.

Conclusion

This study concludes that Sri Lanka's struggle with effective e-governance is primarily rooted in legal uncertainty, lack of institutional integration, and limited public trust. While infrastructure and digital tools exist in various sectors, they are not supported by a consistent legal or policy framework, reducing their impact. India's experience demonstrates that successful e-governance depends on more than just technology. The legal validation of digital identity, enforcement of cyber laws, and the role of the judiciary in legitimizing online processes have all contributed to widespread public confidence. Furthermore, coordinated institutional management and public education campaigns have helped integrate digital services into everyday life.

Sri Lanka can learn valuable lessons by adapting,not merely copying, India's model. Key priorities should include enacting robust digital laws, training government personnel, and building inclusive systems with multilingual support and public feedback channels. Additionally, cooperation between the two countries in digital knowledge-sharing and technical collaboration can accelerate progress. Ultimately, digital governance is a long-term effort that requires legal clarity, administrative commitment, and public engagement. By investing in these areas, Sri Lanka can develop an efficient, accessible, and citizen-centered digital governance system that meets both national and international standards.

References

Basu, Rajesh. (2016). "Legal Foundations of India's E-Governance Revolution." *Indian Journal of Law and Technology* 12 (2): 45–68.

Choudhury, Amit. (2020). "Digital India and the Expansion of Rural Connectivity." *Journal of South Asian Development* 15 (1): 25–49.

Fernando, Malini. (2015). "e-Sri Lanka: Policy Continuity and Political Challenges." *Sri Lanka Journal of Public Policy* 7 (2): 110–128.

Gunawardena, Saman, and Kavita Karunarathna. 2019. "Policy Gaps in Data Protection in Sri Lanka." *Asian Journal of Cyber Law* 3 (1): 72–90.

Jayawardena, U. A., R. A. I. Ranasinghe, and S. Wijayaratna. (2014). "e-Government in Sri Lanka: Current Status, Opportunities, and Challenges." *Int. Journal of Advanced Computer Science & Software Engineering* 4 (6): 357–361.

Karunaratne, K. W. A. D. (2017). "E-Governance in Sri Lanka: A Review of Progress, Issues, and Challenges." *Int. Journal of Advanced Info Systems in Developing Countries* 8 (2): 282–286.

Mukherjee, Ananya. (2015). "Digital Literacy and Government Outreach: India's PMGDISHA Experience." *South Asian Journal of Education Technology* 9 (3): 150–170.

Ratnayake, Chatura. (2022). "Legal Status of Online Public Documents in Sri Lanka." *Journal of Sri Lankan Law* 14 (1): 95–113.

Samarajiva, Rohan, and Suvim Zainudeen. (2008). "e-Sri Lanka: A World Bank–Supported ICT Strategy." *Telecom Policy and Governance* 32 (4): 210–233.

Sharma, Deepak, and Ritu Gupta. (2019). "Rural e-Governance through CSCs: A Model of Legal and Operational Integration." *Indian Journal of Rural Development* 41 (2): 92–112.

Sivarajah, S., and H. Irani. (2016). "E-Governance in Sri Lanka: An

Assessment of Progress and Challenges." *Electronic Journal of Info Systems in Developing Countries* 76 (4): 1–17.

United Nations. (2022). *E-Government Survey 2022: Digital Transformation in Institutions*. New York: UNDESA.

World Bank. (2021). *Sri Lanka Digital Economy and Society Assessment*. Colombo: World Bank.