International Journal of Law, Justice & Statutory Affairs
Volume 1 , Issue 4, 2025

Creating the legal foundation for digital governance

Galang Angga Dian Pradana1, Aristya Windiana Pamuncak2
Faculty of Law
University Syiah Kuala, Banda Aceh, Indonesia

Research Article

Date of Submission: 15-10-2025 **Date of Acceptance: 08-11-2025** **Date of Publication: 26-09-2025**

Abstract
Modern legal frameworks are required since digital technologies are changing government. Sustainable e-government is made possible by constitutional rights, taech-neutral legislation, strong data governance, cybersecurity, and digital inclusion initiatives. Important foundations are provided by targeted legal amendments, such as allowing virtual parliamentary sessions and digital voting. The revolutionary promise of e-governance may be realized with clever regulations that strike a balance between innovation, rights, and responsibility.

Keywords: Data protection, cyber legislation, digital parliament, e-government, and digital governance

Introduction

In order to provide services, boost productivity, enhance transparency, and increase democratic participation, governments around the world are quickly adopting digital technologies [1-3]. Initiatives include blockchain land registries, digital identification systems, virtual legislative sessions, internet portals, automation using artificial intelligence, and more [4-6]. However, establishing strong legal foundations up front is necessary to maximize the advantages of e-governance in a sustainable manner [7, 8]. Important topics and new best practices are examined in this essay.

Legal readiness may either help or hinder the success of e-governance, even if political will is still essential [9]. Modernization is hampered by antiquated regulations that pertain to paper and physical procedures [10]. Risks are increased by unclear data rules [11]. Targeted reforms close these gaps and create an atmosphere that is conducive to the digital revolution of government.

Foundational Legal Frameworks

Constituting digital governance: In order to include digital governance, progressive constitutions are starting to explicitly acknowledge people' rights to effective, transparent e-services [12–14]. Frameworks that facilitate digital service delivery, virtual policymaking, and e-participation gain pace due to constitutional promises.

Enacting tech-neutral laws: Instead of mandating certain technology, laws should promote innovation [15, 16]. Tech-neutral legislation that is centered on ideals and objectives, such as "accessible voting for all," allows implementers to adopt new solutions as technology advances rather than being fixed [17]. It is also crucial to amend out-of-date legislation that include paper, physical presence, etc.

Data governance: The foundation for digitization is provided by explicit data sharing, security, and protection regulations [18, 19]. GDPR and other data privacy rules strike a compromise between user rights and government requirements [20]. Innovation is made possible by open data regulations, which also protect sensitive data [21]. International cooperation is facilitated by provisions for legal cross-border data exchanges [22].

Administrative simplification: Modernization is accelerated by reducing red tape by digitizing bureaucracy, procedures, and identification

requirements [23, 24]. Growth was enhanced when 1500 antiquated laws were repealed in India [25]. Laws pertaining to electronic transactions that facilitate paperless procedures are also essential [26].

Emerging Issues in Digital Governance

Cyber security & risk management: Vulnerabilities increase with the size of digital systems. Resilience is strengthened by laws pertaining to standards, testing, audits, and coordinated responses [27–29]. Accountability for security failures is also required under data protection requirements [30].

It is still essential to address cyber dangers. Digital by default approaches present issues with universal access [31].Through multilingual interfaces, aided e-services, and proactive digital inclusion, laws and regulations must meet the requirements of underprivileged populations [32, 34]. Exclusion is avoided by striking a balance between digitalization and the preservation of non-digital channels. Concerns about content restriction arise when government services go online [35]. Complex trade-offs must be balanced in order to comply with regulations pertaining to transparency, free speech, forbidden content, platform liability, etc. [36]. It is recommended to use multi-stakeholder methods [37].

As AI becomes more prevalent in governance, laws pertaining to automated decision making, algorithmic transparency, and accountability are becoming more and more necessary [38, 39]. One of the biggest challenges is still preventing prejudice and mistakes without inhibiting creativity [40].

Transforming Core Governance Processes

Permitting virtual governance: In order to facilitate digital policymaking, several jurisdictions have changed their laws to permit remote parliamentary sessions and electronic voting [41, 43]. Secure solutions that strike a balance between data security and openness are necessary for virtual sessions. E-governance is furthered by similar public agency changes that increase telework, digital administrative processes, etc.

Public administration regulations and standards for crucial digital public services have been enacted in several nations. These demand cloud adoption, accessibility, interoperability, and other fundamental standards that apply to all agencies. Efficiency and quality are enhanced by standardizing the delivery of digital public services.

Strong digital ID systems that protect privacy are a key component. Laws that specify data security, allowed uses, and proofreading criteria are essential. Blockchain technology is being used to create globally compatible digital IDs, along with other advancements.

Conclusion

Targeted legal changes provide the necessary foundation for successful e-governance, even if political will is still crucial [52]. Responsible innovation is made possible by establishing clear guidelines early on regarding privacy, security, inclusiveness, and responsibility [53]. Sharing best practices for frameworks that strike a balance between agility, rights, and accountability is crucial as digital governance grows internationally [54]. E-governance may really realize its transformational promise as a facilitator of effective, inclusive, and transparent government with wise legal underpinnings.

References

1. Reddick CG, Chatfield AT. Issues with trust, security, and privacy in government customer relationship management (CRM). IGI Global, Public Affairs and Administration: Concepts, Methodologies, Tools, and Applications, c2019, pp. 315–331.
2. Ndou V. E-government: prospects and difficulties for developing nations. The Electronic Journal of Information Systems in Developing Nations. 2004; 18(1):1–24.
3. Wirtz BW, Mory L, Ullrich S. Adoption and success stories of e-government in urban and rural municipalities. Public Administration in the Digital Age International Journal (IJPADA). October 1, 2012, 1(4):1-4.
4. Meijer A. Digitalization and datafication's performative effects on government governance. Edward Elgar Publishing, "Data Governance in the Digital Age," July 30, 2021.
5. es S. Using blockchain technology to enable smart government beyond Bitcoin. at the International Conference on Electronic Governance. p. 253-264; Springer, Cham, c2016.
6. Linders D. Creating a typology for citizen coproduction in the era of social media: From e-government to we-government. Quarterly Government Information. October 1, 2012,

29(4):446-54.
7. Ronaghan SA. Benchmarking e-government: A global perspective. United Nations Publications, December 31, 2002.
8. Gil-García JR, Pardo TA. E-government success factors: Linking useful instruments to theoretical underpinnings. quarterly information from the government. April 1, 2005, 22(2):187-216.
9. Vergari S. Constitutions, laws, and norms: Creating a framework for digital governance. Review of Public Performance and Management. July 4, 2021, 44(5):1165-87.
10. Dawes SS. Digital Age Governance: A framework for research and action in an uncertain future. Quarterly Government Information. April 1, 2010, 27(2):257-64.
11. Zuiderwijk A, Janssen M. Open data policies: A framework for comparison, implementation, and effect. Quarterly Government Information. January 1, 2014, 31(1):17-29.
12. Grimes JM, Bertot JC, and Jaeger PT. Using ICTs to build a culture of transparency: E-government and social media as openness and anti-corruption instruments for society. Quarterly Government Information. July 1, 2010, 27(3):264-71.
13.Reyes AL. Moving parliament to the virtual world: Prospects for e-parliament. Accessible at SSRN 3663444; c2020 April 23.
14. Policy making 2.0: From theory to reality, Ferro E, Loukis EN, Charalabidis Y, Osella M. Quarterly Government Information. October 1, 2013, 30(4):359-68.
15. Janowski T. Evolution of digital government: Transformation to contextualization. Quarterly Government Information. July 1, 2015, 32(3):221-36.
16. Understanding E-Democracy: Government-Led Initiatives for Democratic Reform, Freeman J., Quirke S. 2013, 5(2), JeDEM-eJournal of eDemocracy and Open Government.
17. Socio-technical barriers to open data: Zuiderwijk A, Janssen M, Choenni S, Meijer R, Sheik Alibaks R. Electronic Journal of e-Government. 2012;10(2):156-172.
18.Hintze M. Viewing the GDPR via a de-identification lens: A tool for compliance, explanation, and consistency. International Data Privacy Law. 2018 Feb 1;8(1):86-101.
19.Janssen M, Charalabidis Y, Zuiderwijk A. Benefits, adoption hurdles and misconceptions of open data and open government. Information systems management. 2012;29(4):258-68.
20.Chander A, Le U. Data nationalism. Emory LJ. 2015;64:677.
21.Madsen CØ, Berger JB. Digitalization and public sector reforms. Palgrave Macmillan, Cham; c2020 Jun10.
22.Mazumdar S. Impact of e-government development on administrative efficiency and corruption: A cross-country research. Electronic Government, an International Journal. 2018;14(3):213-40.
23.Cullen R. New directions for electronic government: reforming government via technology. Perspectives on Global Development and Technology; c2020 Mar 4. p. 71-87.
24.Van Eeten M, Bauer JM. Emerging challenges to internet security: incentives, externalities and policy consequences. Journal of Contingencies and Crisis Management. 2009 Sep;17(4):221-32.
25.Floridi L. Governing artificial intelligence via ethics by design. Philosophy & Technology. 2021 Jun;34(2):287-95.
26.Klimburg A, ed. National cyber security framework handbook. NATO CCD COE Publication, Tallinn; c2012.
27.Tankard C. What the GDPR entails for companies. Network Security. 2016 Jun 1;2016(6):5-8.
28.Helbig N, Gil-García JR, Ferro E. Understanding the complexity of electronic government: Implications from the digital divide literature. Quarterly Government Information. 2009 Jan 1;26(1):89-97.
29.Alruwaie M, El-Haddadeh R, Weerakkody V. A framework for assessing citizens' expectations and satisfaction regarding continuous intention to utilize e-government services. In Proceedings of the 18th annual international conference on digital government research; c2017. p. 572-576.
30.Checchi RM, Sevcikova H, Nardo M, de Beni E. ICT accessibility for everybody and eInclusion in the new digital economy. Publications Office of the European Union; c2012 Nov 1.
31.Cullen R, Cullen C. Digitalization and public sector change. In The Routledge Handbook of Service Research Insights and Ideas. Edward Elgar Publishing; c2018.
32.Bertot JC, Jaeger PT, Grimes JM. Promoting openness and accountability using ICTs, social media, and big data. International Journal of E-Politics (IJEP). 2012 Jan 1;3(1):78-90.

33.Pickard VK, Yang G. Media activism in the digital age: Social movements and e-campaigns. The Routledge Handbook of Security, Conflict, and Media. p. 101–11. Abingdon: Routledge, c2020.
34. Desouza K.C. The potential and challenges of using artificial intelligence in governance. IBM Center for the Business of Government, July 9, 2018, pp. 1–32.
35. Williams MN, Moses LF, and Zalnieriute M. the automation of government decision-making and the rule of law. Review of Modern Law. May 2019, 82(3), 425-56.
36.AI4People: an ethical framework for a decent AI society: possibilities, hazards, principles, and suggestions Floridi L, Cowls J, Beltrametti M, et al. Machines and Minds. December 2018, 28(4):689-707.
37. Horst M, Krasodomski-Jones A. Ensuring elected representatives have their proper democratic position in the digital public sphere: The digital route to representative governance. Democracy Reporting International, Nov. 1, 2019, pp. 1-A4, 38. Coughlan S. Is it possible that virtual parliaments will become commonplace? BBC News, April 22, 2020. Accessed January 28, 2023.
39. Goodman JW, Ignacio J. Parliament in the Internet era. 21st-century Parliament and Democracy. Hart Publishing, 2015, pp. 227–242.
40. Guler A, Pardo TA, Burke GB, Gil-García JR. Determining the factors that influence government cross-border information sharing activities. System Sciences (HICSS), 43rd Hawaii International Conference, 2010. IEEE, January 1, 2010, pp. 1–10.
41. Whitley EA, Kjaergaard A, Gal U. Who do you consider yourself to be? An examination of the intricate relationship between identity, identification, and information systems. Journal of Information Systems in Europe. February 2014, 23(1):17-35.
42. George C, Hazard JT, Wigan M. Security, identity, and privacy. Australian Journal of Digital Economy and Telecommunications. December 19, 2016, 4(4):109-18.
43. Snijkers K, Rotthier S, Janssen D. Will they come if you build it? An empirical assessment of local government data visualization. Quarterly Government Information. April 1, 2020, 37(2):101477.