



E-ISSN: 2790-0681
P-ISSN: 2790-0673
IJLJJ 2024; 4(1): 06-08
Received: 15-10-2023
Accepted: 19-11-2023

Odiljon Tojiev
Researcher, Tashkent State
University of Law, Tashkent,
Uzbekistan

Laying the legal groundwork for digital governance

Odiljon Tojiev

DOI: <https://doi.org/10.22271/2790-0673.2024.v4.i1a.86>

Abstract

Digital technologies are transforming governance, necessitating updated legal frameworks. Constitutional rights, tech-neutral laws, robust data governance, cybersecurity, and digital inclusion measures enable sustainable e-governance. Targeted legislative reforms, like permitting virtual parliamentary sittings and digital voting, provide important foundations. With astute rules balancing innovation, rights and accountability, the transformative potential of e-governance can be fulfilled.

Keywords: Digital governance, e-government, cyber law, data protection, digital parliament

Introduction

Governments globally are rapidly embracing digital technologies to deliver services, increase efficiency, improve transparency and expand democratic participation ^[1-3]. Initiatives span online portals, automation using artificial intelligence, virtual parliamentary sessions, digital identity schemes, blockchain land registries and more ^[4-6]. However, optimizing the benefits of e-governance sustainably requires laying robust legal foundations upfront ^[7, 8]. This article examines key issues and emerging best practices.

While political will remains crucial, legal preparedness can accelerate or inhibit e-governance success ^[9]. Outdated laws referencing paper and physical processes hamper modernization ^[10]. Unclear data rules raise risks ^[11]. By addressing such gaps, targeted reforms create an enabling environment for digital transformation of governance.

Foundational Legal Frameworks

Constituting digital governance: Progressive constitutions are beginning to expressly recognize citizens' rights to efficient, transparent e-services, embedding digital governance ^[12-14]. Constitutional commitments create momentum for frameworks enabling virtual policymaking, digital service delivery and e-participation.

Enacting tech-neutral laws: Legislation should avoid prescribing specific technologies, allowing innovation ^[15, 16]. Tech-neutral laws focused on principles and goals - like "accessible voting for all" - give implementers flexibility to use new solutions as technology evolves rather than getting locked in ^[17]. Amending outdated laws referencing paper, physical presence etc. is also essential.

Data governance: Clear data protection, sharing and security rules provide the bedrock for digitalization ^[18, 19]. Data privacy laws like GDPR balance user rights with government needs ^[20]. Open data policies enable innovation while securing sensitive information ^[21]. Provisions for lawful cross-border data flows facilitate global collaboration ^[22].

Administrative simplification: Cutting red tape by streamlining bureaucracies, workflows and identification requirements through digitization speeds modernization ^[23, 24]. India's abolition of 1500 archaic laws accelerated growth ^[25]. Electronic transactions laws enabling paperless processes are also key ^[26].

Emerging Issues in Digital Governance

Cyber security & risk management: As digital systems grow, so do vulnerabilities. Laws on standards, testing, audits and coordinated responses strengthen resilience ^[27-29]. Data protection obligations also compel accountability for security breaches ^[30].

Correspondence Author:
Odiljon Tojiev
Researcher, Tashkent State
University of Law, Tashkent,
Uzbekistan

Addressing cyber risks remains an ongoing imperative.

Universal access challenges arise with digital by default models^[31]. Laws and policies must address needs of disadvantaged groups through multi language interfaces, assisted e-services and proactive digital inclusion^[32, 34]. Balancing digitization with retention of non-digital channels prevents exclusion. As government services move online, content regulation issues emerge^[35]. Rules on transparency, free expression, prohibited material, platform liability etc. require balancing complex tradeoffs^[36]. Multi-stakeholder approaches are advocated^[37].

Laws on automated decision making, algorithmic transparency and accountability are increasingly needed as AI grows in governance^[38, 39]. Preventing bias and errors, without stifling innovation, remains a key challenge^[40].

Transforming Core Governance Processes

Permitting virtual governance: Some jurisdictions have implemented legislative changes to enable digital policymaking, like allowing remote parliamentary sittings and e-voting^[41, 43]. Virtual sessions require secure solutions balancing transparency with data protections. Similar public agency reforms expanding telework, digital administrative procedures etc. further e-governance.

Many countries have passed public administration laws and standards for essential digital public services. These mandate accessibility, interoperability, cloud adoption and other baseline requirements applicable across agencies. Standardizing digital public service delivery promotes quality and efficiency.

A major foundation is robust digital ID systems that preserve privacy. Laws defining proofing requirements, permitted uses and data protections are vital. Globally interoperable digital IDs using blockchain and other innovations also emerging.

Conclusion

While political will remains vital, targeted legislative reforms lay essential groundwork for sustainable e-governance^[52]. Setting clear rules on privacy, security, inclusion and liability at the outset enables responsible innovation^[53]. As digital governance expands globally, sharing best practices on frameworks balancing agility, rights and accountability remains key^[54]. With astute legal foundations, e-governance can genuinely fulfill its transformative potential as an enabler of efficient, inclusive and transparent governance.

References

1. Chatfield AT, Reddick CG. Customer relationship management (CRM) in government: Privacy, security, and trust issues. In *Public affairs and administration: Concepts, methodologies, tools, and applications* IGI Global; c2019. p. 315-331.
2. Ndou V. E-government for developing countries: opportunities and challenges. *The Electronic Journal of Information Systems in Developing Countries*. 2004;18(1):1-24.
3. Wirtz BW, Mory L, Ullrich S. E-Government in cities and rural municipalities: Comparing adoption and success stories. *International Journal of Public Administration in the Digital Age (IJPADA)*. 2012 Oct 1;1(4):1-4.
4. Meijer A. *Governing the government: The performative effects of digitalization and datafication*. Data Governance in the Digital Age. Edward Elgar Publishing; c2021 Jul 30.
5. Ølnes S. Beyond Bitcoin enabling smart government using blockchain technology. In *International Conference on Electronic Government*. Springer, Cham; c2016. p. 253-264.
6. Linders D. From e-government to we-government: Defining a typology for citizen coproduction in the age of social media. *Government Information Quarterly*. 2012 Oct 1;29(4):446-54.
7. Ronaghan SA. *Benchmarking e-government: A global perspective*. United Nations Publications; c2002 Dec 31.
8. Gil-García JR, Pardo TA. E-government success factors: Mapping practical tools to theoretical foundations. *Government information quarterly*. 2005 Apr 1;22(2):187-216.
9. Vergari S. Norms, statutes, and constitutions: Establishing a digital governance framework. *Public Performance & Management Review*. 2021 Jul 4;44(5):1165-87.
10. Dawes SS. Governance in the digital age: A research and action framework for an uncertain future. *Government Information Quarterly*. 2010 Apr 1;27(2):257-64.
11. Zuiderwijk A, Janssen M. Open data policies, their implementation and impact: A framework for comparison. *Government Information Quarterly*. 2014 Jan 1;31(1):17-29.
12. Bertot JC, Jaeger PT, Grimes JM. Using ICTs to create a culture of transparency: E-government and social media as openness and anti-corruption tools for societies. *Government Information Quarterly*. 2010 Jul 1;27(3):264-71.
13. Reyes AL. Moving parliament to the virtual world: Prospects for e-parliament. Available at SSRN 3663444; c2020 Apr 23.
14. Ferro E, Loukis EN, Charalabidis Y, Osella M. Policy making 2.0: From theory to practice. *Government Information Quarterly*. 2013 Oct 1;30(4):359-68.
15. Janowski T. Digital government evolution: From transformation to contextualization. *Government Information Quarterly*. 2015 Jul 1;32(3):221-36.
16. Freeman J, Quirke S. Understanding E-Democracy: Government-Led Initiatives for Democratic Reform. *JeDEM-eJournal of eDemocracy and Open Government*, 2013, 5(2).
17. Zuiderwijk A, Janssen M, Choenni S, Meijer R, Sheikh Alibaks R. Socio-technical impediments of open data. *Electronic Journal of e-Government*. 2012;10(2):156-172.
18. Hintze M. Viewing the GDPR through a de-identification lens: A tool for compliance, clarification, and consistency. *International Data Privacy Law*. 2018 Feb 1;8(1):86-101.
19. Janssen M, Charalabidis Y, Zuiderwijk A. Benefits, adoption barriers and myths 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 transformations*. Palgrave Macmillan, Cham; c2020 Jun

- 10.
22. Mazumdar S. Impact of e-government development on administrative efficiency and corruption: A cross-country study. *Electronic Government, an International Journal*. 2018;14(3):213-40.
23. Cullen R. New directions for electronic government: transforming government through technologies. *Perspectives on Global Development and Technology*; c2020 Mar 4. p. 71-87.
24. Van Eeten M, Bauer JM. Emerging threats to internet security: incentives, externalities and policy implications. *Journal of Contingencies and Crisis Management*. 2009 Sep;17(4):221-32.
25. Floridi L. Governing artificial intelligence through ethics by design. *Philosophy & Technology*. 2021 Jun;34(2):287-95.
26. Klimburg A, ed. National cyber security framework manual. NATO CCD COE Publication, Tallinn; c2012.
27. Tankard C. What the GDPR means for businesses. *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. *Government Information Quarterly*. 2009 Jan 1;26(1):89-97.
29. Alruwaie M, El-Haddadeh R, Weerakkody V. A framework for evaluating citizens' expectations and satisfaction toward continued intention to use 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 all 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 transformation. In *The Routledge Handbook of Service Research Insights and Ideas*. Edward Elgar Publishing; c2018.
32. Bertot JC, Jaeger PT, Grimes JM. Promoting transparency and accountability through 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. *Routledge Handbook of Media, Conflict and Security*. Abingdon: Routledge; c2020. p. 101-11.
34. Desouza KC. Delivering artificial intelligence in government: Challenges and opportunities. *IBM Center for The Business of Government*; c2018 Jul 9. p. 1-32.
35. Zalnieriute M, Moses LF, Williams MN. The rule of law and automation of government decision-making. *Modern Law Review*. 2019 May;82(3):425-56.
36. Floridi L, Cows J, Beltrametti M, *et al.* AI4People-an ethical framework for a good AI society: opportunities, risks, principles, and recommendations. *Minds and Machines*. 2018 Dec;28(4):689-707.
37. Horst M, Krasodonski-Jones A. The digital road to representative government: Ensuring elected representatives their rightful democratic place in the digital public sphere. *Democracy Reporting International*; c2019 Nov 1. p. 1-A4.
38. Coughlan S. Could virtual parliaments become the norm? *BBC News*; c2020 Apr 22. Accessed 2023 Jan 28. <https://www.bbc.com/news/technology-52380017#:~:text=The%20coronavirus%20pandemic%20has%20forced,place%20under%20social%2Ddistancing%20rules.>
39. Goodman JW, Ignacio J. Parliament in the age of the Internet. In *Parliament and Democracy in the Twenty-First Century*. Hart Publishing; c2015. p. 227-242.
40. Gil-García JR, Guler A, Pardo TA, Burke GB. Trust in government cross-boundary information sharing initiatives: Identifying the determinants. *System Sciences (HICSS)*, 2010 43rd Hawaii International Conference on. IEEE; c2010 Jan 1. p. 1-10.
41. Whitley EA, Gal U, Kjaergaard A. Who do you think you are? A review of the complex interplay between information systems, identification and identity. *European Journal of Information Systems*. 2014 Feb;23(1):17-35.
42. George C, Hazard JT, Wigan M. Privacy, identity and security. *Aus. J of Telecommunications and the Digital Economy*. 2016 Dec 19;4(4):109-18.
43. Janssen D, Rothier S, Snijders K. If you build it, will they come? An empirical evaluation of data visualization in local government. *Government Information Quarterly*. 2020 Apr 1;37(2):101477.