The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

"DIGITAL GOVERNANCE AND ADMINISTRATIVE EFFICIENCY: A LEGAL ANALYSIS OF THE IT ACT 2000 IN THE VISION OF VIKSIT BHARAT 2047"

~ Chandan Sha*

Abstract:

This paper examines how the enactment of the Information Technology Act 2000 transformed governance in India, shaping India's e-governance landscape and administrative efficiency in the context of the government's "Viksit Bharat 2047" vision. This paper traces the evolution of e-governance and explains the gap between the legislation and its implementation with various cases which are notably shaping e-governance in India. We assess the impact of these reforms on administrative efficiency and citizen-centric governance, noting evidence that direct benefit transfers and other e-governance measures have saved government resources and accelerated service delivery. A brief comparative perspective discusses global digital-ID and e-governance models (e.g. Estonia, EU)[1]. Finally, we address challenges – notably data privacy, security vulnerabilities, and the persistent digital divide – and review India's new data protection regime (DPDP Act 2023) and other reforms in progress.

Keywords: Viksit Bharat 2047; Digital governance; IT Act, 2000; DPDP Act 2023; Administrative Efficiency.

* Student of 5-year B.B.LL.B. (Hons.), Semester IX, Indian Institute of Legal Studies, Siliguri, Email: chandansha367@gmail.com

[1] Coley Felt & Will LaRivee, *Exploring the Global Digital ID Landscape,* ATLANTIC COUNCIL GEOTECH CTR. (July 10, 2025), https://www.atlanticcouncil.org/in-depth-research-reports/report/exploring-the-global-digital-id-landscape/ (last visited Aug. 18, 2025).

1. INTRODUCTION TO DIGITAL GOVERNANCE IN INDIA

As per Dr. APJ Abdul Kalam, the former President of India- "A transparent, smart e-Governance with seamless access, secure and authentic flow of information crossing the interdepartmental barrier and providing a fair and unbiased service to the citizen."[2] is the vision for the future of e governance in India.

In layman language, Digital governance means the use of information and communication technologies (ICT) by government to provide services, engage citizens, and properly manage public records. In India, Digital governance transformation has evolved over the past two decades. Before 2000, the e governance in India was only limited to the government department but after the enactment of the IT act in 2000, it marked the beginning of proper e governance in India. It was also after the introduction of the National e governance plan in 2006 that highlighted the importance of online filing and validation of e- records. In 2015, the government launched Digital India, a flagship programme "to transform India into a digitally empowered society and knowledge economy"[3] Various initiatives are taken by the government, like digital infrastructure development, e-services platforms, and universal connectivity, to make India 'The Digital India' by expanding access to online services like Aadhaar, UPI, Digi-Locker, UMANG, JAM Trinity, e-Office. Administrative efficiency integrated with transparency, inclusivity, resilience was a problem for the proper e governance so the legislature in the year 2023 enacted the Digital personal data protection Act 2023. The government explicitly links digital governance to its long-term vision: "with a clear focus on realising the vision of a 'Viksit Bharat' i.e. Developed India by 2047," India is laying out plans to empower citizens via welfare programs, skill development, and inclusive digital services.[4]

Technology is viewed as a catalyst for "innovation" and "good governance" – enhancing transparency, efficiency and citizen participation through e-government platforms and digital payments.[5]

In short, India is on its path in achieving the goal of being 'Digital India' while also aligning with the vision of Viksit Bharat 2047.

---

[2] *E-Governance,* INSIGHTS ON INDIA, https://www.insightsonindia.com/governance/e-governance/ (last visited Aug. 20, 2025).
[3] Gary Kovacs, *Tracking Our Online Trackers*, TED TALKS (Feb. 2012), https://www.ted.com/talks/gary_kovacs_tracking_our_online_trackers (last visited Aug. 18, 2025).
[4] *About Us,* DIGITAL INDIA, MINISTRY OF ELECTRONICS & INFO. TECH., GOV'T OF INDIA, https://www.digitalindia.gov.in/about-us/ (last visited Aug. 20, 2025).
[5] *Id.*

2. EVOLUTION OF E-GOVERNANCE IN INDIA

E-governance in India has been a gradual process brought about by technological advances, administrative decisions and legal acceptance of e-processing. This development could be characterised into three periods, namely, pre-2000 computerisation era, legal consolidation pursuant to the IT Act (2000 - 2010), and growth through flagship programmes (2010 onwards).

2.1 Pre-2000: Foundations of Computerisation

Before the 2000 it was only e-governance were in the area of internal computerisation of government departments. The National Informatics Centre (NIC) was founded in 1977 signalling the first institutionalised effort towards digital governance. The introduction of NICNET in 1987 offered satellite communications infrastructure, which supported interconnection of government offices in the nation. [6] The main use of technology in this stage involved record-keeping, economic observation and data-heavy processes such as elections and census activities. The pilot projects comprised the computerisation in defence services, railway reservation and tax administration.[7] These efforts illustrated the efficiencies achievable when using technology but failed to provide a broad-based legal framework to facilitate the use of electronic records or transactions.

2.2 2000–2010: The IT Act and Legal Recognition

The development of IT Act, 2000 was a breakthrough or departure point in electronic governance as the information technology was now considered as a form of electronically recognised governance. Demands of security issues and digital electronic signatures were legalised in Indian law for the first time (Sections 4-7) of IT Act, 2000, enabling Indians and businesses to carry out electronic transactions with government bodies.[8]

The 2008 Amendment further opened out the Act to focus on cybersecurity threats, recognise electronic signatures, as well as offer the provisions of data protection and the intermediary liability. This was also the time when the National e-Governance Plan (2006) was introduced,

---

[6] *About NICNET,* NATIONAL INFORMATICS CENTRE, MINISTRY OF ELECTRONICS & INFO. TECH., https://www.nic.in (last visited Aug. 18, 2025).
[7] B.K. Gairola, *Evolution of e-Governance in India,* 12 J. GOVERNANCE 45, 48 (2016).
[8] The Information Technology Act, 2000, §§4–7, No. 21, Acts of Parliament, 2000 (India).

which identified 27 Mission Mode Projects in areas including land records, banking, taxation and agriculture etc.[9]

2.3 2010 Onwards: Expansion through Digital India

Greater-scale, citizen-centric e-governance started when the Digital India programme was launched in 2015. The programme was intended to become the of digital infrastructure as a service to all citizens, governance and services on demand and to empower citizens digitally.[10]

Major projects were Aadhaar-based identity, Unified Payments Interface (UPI), Digi-Locker, UMANG, the state-level service delivery platforms. By 2024, more than 12 billion UPI transactions were taking place each month and Aadhaar was being used to open hundreds of millions of banking accounts via the Jan Dhan scheme.[11]

The adoption of the India Stack of various APIs that include Aadhaar, UPI, Digi-Locker, and e-KYC has enabled India to become a global leader in scalable digital public infrastructure.[12]

3. LEGAL AND INSTITUTIONAL FRAMEWORK OF THE IT ACT, 2000

The core of India's digital governance is the Information Technology Act, 2000 (i.e. IT Act 2000) – the country's primary cyberlaw. The IT Act, 2000 was enacted to create a *"legal framework for electronic governance by giving recognition to electronic records and digital signatures"* [13] It was India's response to the UNCITRAL Model Law on Electronic Commerce (1996) and the recognition that ICT-driven transactions needed legal backing.

3.1. Section 4 – Legal Recognition of Electronic Records:[14]

Section 4 makes an electronic record or copy thereof in writing and on paper sufficient, as per law. This "functional equivalence" is fundamental: it means e-forms and scanned documents have the same legal status as paper, enabling all manner of transactions to go digital. As an example, electronically signed tax return or a license application is legally binding under Sec. 4 (as amended). This has come as an influence of the UN Model Law on Electronic Commerce

---

[9] *National e-Governance Plan,* MINISTRY OF ELECTRONICS & INFO. TECH., https://www.meity.gov.in (last visited Aug. 18, 2025).
[10] *Digital India Programme,* GOVERNMENT OF INDIA, https://www.digitalindia.gov.in (last visited Aug. 18, 2025).
[11] *UPI Data,* RESERVE BANK OF INDIA, https://www.rbi.org.in (last visited Aug. 18, 2025).
[12] Nandan Nilekani, *Building India Stack*, 51 ECON. & POL. WKL. 50, 52 (2016).
[13] Hemant More, *Information Technology Act, 2000: A Backbone of Indian Digital Revolution,* THE LEGAL QUOTIENT (July 29, 2024), https://thelegalquotient.com (last visited Aug. 18, 2025).
[14] The Information Technology Act, 2000, §4.

and this is paramount to the objectives of the IT Act eg. facilitating the efficient delivery of Government services.

3.2. Section 6 – Electronic Records and Signatures in Government:[15]

Section 6 gives a ground for a effectively *mandating* e-governance. As long as one can electronically express the act through form that was prescribed by the government, then that act can fulfill the requirements of a law that dictates a method of performance of submitting an application, issuing a permit and making a payment. In practice, Sec. 6 compels government bodies to accept e-submission of forms, e-issuance of licenses, and e-payments. Thus, many citizen–government interfaces (income tax e-filing, company incorporation, land registry, etc.) became possible due to this legal rule. The legislative intent was to "facilitate electronic filing of documents with the Government agencies" (Preamble) and Sec. 6 operationalizes that. Procedural rules under Sec. 6 (by Notification) define how agencies must implement e-services, and refusal to accept a valid e-filing can be challenged as contrary to law.

3.3. Section 7 – Retention of Electronic Records:[16]

Section 7 deals with record retention: it prescribes that if law requires certain documents to be kept, that requirement is satisfied if the information is retained in electronic form that is accessible and usable over time. It will also mandate some information (origin, destination, time) be affixed to electronic records to maintain evidence integrity. This section invites governments and courts to consider archived e-records equal to physical records where they have been properly archived.

3.4. Section 66 – Computer-Related Offenses:[17]

Section 66 is a general penal provision making it an offense (punishable by up to 3 years jail or fine) to "dishonestly or fraudulently" do any act referred to in Sec. 43[18] (which covers various computer misuses). It thus criminalizes hacking, data theft, virus attacks etc. Section 66[19] (and related sections 66C-66F)[20] grant the government legal tools to secure cyberspace

[15] *Id* §6.
[16] *Id* § 7.
[17] *Id* § 66.
[18] *Id* § 43.
[19] *Id* § 66.
[20] *Id* §§ 66C-66F.

and thus indirectly protect e-governance systems from abuse. The Sections 66C (identity theft), 66E (privacy violation- about intimate images) were added in 2008. The severely prescribed Section 66A (offensive messages) was declared invalid in Shreya Singhal but Section 66C-66E (identity, privacy violations) is still in the law yet it is rarely used.

For example, 66E had influenced policy on protecting bio-metric data under the Aadhaar Act. Section 66 and its following sections impose liabilities to discourage cybercrimes that could undermine trust in digital governance.

3.5. Section 79 – Liability of Intermediaries (Safe Harbor):[21]

Section 79 gives immunity to intermediaries (e.g. ISPs, telecoms, social media platforms), which means that they will not be held liable or responsible in the event whereby the content that they host is considered third-party. Section 23[22] states that, an intermediary shall not be liable for third party information, data, and communication links. This liability is under the condition formulated in the preceding section. Such a safe harbor is crucial to enable digital services to work without being obliged to pre-screen all the user content. The Court in the *Shreya Singhal* case[23] clarified that there is no active role that intermediaries are bound to perform in respect to filtering content without a court or a government direction and thus the scope of Sec. 79 was reinforced.

4. JUDICIAL INTERPRETATIONS

Indian Judiciary has played an important role in the shaping of boundaries of digital governance especially in terms of the underlying rights of a citizen and the interest of the state in terms of regulations. Notwithstanding its progressive nature at the time it was enacted, the IT Act had extensive loopholes that had to be filled through jurisprudence. Courts and in particular, the Supreme Court have explained the points of collision between digital rights and free speech, privacy, and due process.

[21] The Information Technology Act, 2000, § 79, No. 21, Acts of Parliament,2000 (India).
[22] *Id* § 23.
[23] *Shreya Singhal v. Union of India,* (2015) 5 SCC 1.

4.1 Shreya Singhal v. Union of India (2015)[24]

In this case the supreme court declared the Section 66A of the IT Act as unconstitutional which criminalised speech on the internet that was found to be offensive or annoying but the Court found it to be against Article 19(1)(a) of the Constitution.

It was after this case that the court emphasized that the freedom of expression should be protected even in cyberspace. It also provided further certainty on intermediary liability under Section 79 by providing that a platform will only respond to remove the content when presented with actual knowledge of an order of a court or government body. Through protection of expression, the Court enabled the efficiency of administrative functions of digital governance not to result in arbitrary censorship.

4.2 Justice K.S. Puttaswamy v. Union of India (2017)[25]

In this case the Supreme Court upheld that the "Right to privacy as a fundamental right" under Article 21 of the constitution of India. The Court justified Aadhaar in simplifying the delivery of welfare programs - especially by eliminating duplicate and leakage of subsidies and hence streamlining the administrative systems. But it invalidated some clauses that granted people to utilise the Aadhaar in the private sector and restricted state custody of the data. The ruling illustrated that effectiveness in ruling cannot be achieved by engaging in excessive monitoring.

4.3 Anuradha Bhasin v. Union of India (2020)[26]

In this case, the Supreme Court dealt with arbitrary internet shutdown in Jammu & Kashmir after the scrapping of Article 370.[27] The Court reasoned "that freedom of speech, as well as trade and commerce in terms of Article 19(1) (a) and 19(1) (g), require access to the internet and therefore it is subject to the right to freedom of speech and to trade and commerce."

The Court considered that the "fundamental rights cannot be superseded by the administrative actions, such as shutdowns, by focusing on proportionality and regularly reviewing the

[24] Shreya Singhal, supra note 23.
[25] *K.S. Puttaswamy v. Union of India,* (2017) 10 SCC 1; (2019) 1SCC 1.
[26] *Anuradha Bhasin v. Union of India,* (2020) 3 SCC 637.
[27] *Id.*

limitations so that as much as possible, the non-infringement of the fundamental rights is not possible."

The effective governance in the digital age must have lawful, transparent and accountable governance structures that are not arbitrary. Taken together these judicial adjudications have made it such that digital governance in India is no longer merely dictated by the statutory law, but also constitutional principles of individual liberty, equality and accountability.

5. CASE STUDIES OF IMPLEMENTATION

The consequences of evaluating the functioning of the legal frameworks can best be examined with reference to the legal practice through different examples. A number of showcase projects demonstrate the role played by the IT Act in empowering project whose outcomes have direct influence on the citizens, as well as the interdependence between digital governance and the ease or efficiency in the administration.

5.1 Aadhaar and Direct Benefit Transfers (DBT)

The world largest identity project is the Aadhaar programme anchored on biometric identification. Aadhaar has enabled the Direct Benefit Transfer mechanism wherein the subsidies and the welfare payments are directly put to the bank accounts of the recipients. This has minimised leakages, got rid of ghost beneficiaries as well as increased transparency.[28] As an example, in the Public Distribution System, Aadhaar-enabled authentication reduced ration card duplication and allowed the government to achieve cost savings as well as citizens to access their supplies more rapidly. In this case, e-records we logged in by law as given under the IT Act was fundamental in the approving of Aadhaar-linked transactions. Notably, it depicts the fact that administrative efficiency is enhanced as legal structures provide reliability and expertise in digital systems.

5.2 Centralised Public Grievance Redress and Monitoring System (CPGRAMS)

Centralised Public Grievance Redress and Monitoring System **(**CPGRAMS) is an Internet application whereby individuals file complaints about government departments. It has been

[28] *Aadhaar Dashboard,* UNIQUE IDENTIFICATION AUTHORITY OF INDIA (UIDAI), https://uidai.gov.in (last visited Aug. 18, 2025).

combined with the IT Act provisions of electronic communication and record-keeping. The system enables complaints to be tracked in real time and those who take responsibility to be accountable in confirmation of the complaints by departmental officers.[29] It portrays a direct relation between e-governance and efficiency in the administration. Previously, grievance redress was slow, fragmented, and paper-heavy. CPGRAMS has minimized delays, central monitoring, and it has offered data analysis in determining the root causes of systems problems in governance

5.3 e-Office

The e-Office initiative in the National e-Governance Plan digitises movement of files, approvals and correspondence in government departments. Because the files are removed in the form of paper, it removes delays and makes it possible to work remotely.[30] The e-Office also facilitated the succession of administrative operation during the ongoing COVID-19 pandemic, which further proves its significance in ensuring the continuity of Government machinery. The legal basis of the idea finds its backing in the Section 6 of the IT Act that gives support to an electronic record in official communications.

5.4 JAM Trinity: Jan Dhan, Aadhaar, Mobile

The JAM Trinity is constituted of Jan Dhan bank accounts, Aadhaar identity and mobile connectivity to deliver benefits and services directly to the citizens. It has been at the heart of financial inclusion, which facilitated direct LPG subsidy transfer and COVID-19 relief packages.[31]

This integration is an operationalisation of digital governance visions - minimised bureaucracy, minimised cost, and inclusion. On an administrative front, JAM has proved to be revolutionary in terms of delivering at the last mile where legal and digital infrastructure go hand in hand ensuring efficiency.

---

[29] *CPGRAMS Portal,* DEPARTMENT OF ADMINISTRATIVE REFORMS, https://pgportal.gov.in (last visited Aug. 18, 2025).
[30] *e-Office Mission Mode Project*, MINISTRY OF ELECTRONICS & INFO. TECH., https://meity.gov.in (last visited Aug. 18, 2025).
[31] *Jan Dhan–Aadhaar–Mobile Trinity,* NITI AAYOG, https://www.niti.gov.in (last visited Aug. 18, 2025).

6. CHALLENGES AND CRITICISM

6.1 The Digital Divide

At present times, there is an unequal access to digital infrastructure. India TRAI data indicates that rural India continues to be a problem area for penetration of the internet with serious gender disparities to access to smartphones and connectivity.[32] This digital divide negates or hampers the inclusivity of the governance as the participants of digital schemes are limited to those who have a reliable digital access. Administrative efficiency is not a metric that can be limited to measuring speed of delivery but it should also include equity in access

6.2 Outdated Provisions of the IT Act

The IT Act has failed to adapt to newer technologies like artificial intelligence, blockchain and cross-border data flows even after its amendment in 2008.[33] Cyber offenses have not been sufficiently provided in granting laws to sophisticated cyber-attacks such as ransomware or phishing scams. The discrepancy between the law and the technology reduces administrative efficiency since laws become outdated to the extent that systems cannot respond to emerging threats.

6.3 Cybersecurity Concerns

Shifting of government functions to the internet has led to serious dangers associated with hacking of computer databases, computer-based identity systems, and online financial transactions. High-profile security breaches related to Aadhaar data and ransomware attacks on government servers have led some to question how robust India cybersecurity infrastructure is as a result of these attacks fund[34] General public will lose their trust from the government, if there is any lack in effective legal safeguards, technological investments and administrative efficiency.

6.4 Overreach and Privacy Concerns

Critics say that the Aadhaar system and data storage poses a risk of over-surveillance. The Supreme Court in Puttaswamy curtailed such access by the private sector, although there are

[32] TELECOM REGULATORY AUTHORITY OF INDIA, PERFORMANCE INDICATORS REPORT (2023).
[33] Apar Gupta, *Reforming India's IT Act,* 16 IND. J.L. & TECH. 215, 218 (2020).
[34] MINISTRY OF ELECTRONICS & INFO. TECH., CERT-IN ANNUAL REPORT 2022 (2023).

still ambiguities with regard to access of such data by the private sector. Under Section 7 of the Act[35] lists situations where data can be processed without consent – for instance, when required by law, in compliance with court orders, or when data is *"*voluntarily provided*"* by principals.[36] As per, Section 7(b)[37] which permits government agencies to process data without purpose limitations, as long as the data principal has freely given it (for example, submitting information on a government form). The aim is to let states use data to achieve public objectives. There has been a difference in opinion and ongoing debates on how can personal rights be aligned with efficiency.

7. DATA PROTECTION AND THE DPDP ACT, 2023

Enactment of the Digital Personal Data Protection Act (DPDP), 2023, is a milestone in India trying to integrate its law with the digital age. It directly deals with the privacy issues defined in Puttaswamy and the loophole that was left by the IT Act. The DPDP Act brings with it the component of the lawfulness of processing, collecting data with consent, and giving rights to individuals, including the right to correction and erasure of data.[38] It also sets responsibilities on data fiduciaries and gives the government power to lay down norms of localising data. The DPDP Act has a twofold role in the angle of administrative efficiency. On the one hand, it builds citizen confidence in the online environments as it requires protection of citizens data, without which scale is impossible. On the other hand, it generates compliance requirements that may have the effect of slowing innovation or raising operational costs to small companies[39] More importantly, the Act is indicative of an approach to the legal system in India that now treats data as both economic property and a citizenship-related right. In its attempt to establish a governance framework in which efficiency is not alien to accountability, it complements the IT Act.

7.1 DPDP Act vs. IT Act, 2000- A Paradigm Shift

A Paradigm Shift means fundamental change in the approach of a Digital Personal Data Protection Act, 2023 (DPDP Act) it aims to balance privacy with the security of the state. Under the IT Act/SPDI Rules, only *"sensitive personal data"* held by certain private entities was

[35] The Digital Personal Data Protection Act, 2023, § 7, No. 22, Acts of Parliament,2023 (India).
[36] Bharat Manwani & Abhiraj Rana, *The Right to (Pry)-vacy: Understanding India's Dystopian Data Protection Legislation,* JILP BLOG (Feb. 12, 2024), https://jilpblog.com (last visited Aug. 18, 2025).
[37] The Digital Personal Data Protection Act, 2023, § 7(b), No. 22, Acts of Parliament,2023(India).
[38] The Digital Personal Data Protection Act,2023, No. 22, Acts of Parliament,2023 (India).
[39] Id. §§ 5–10.

covered. But DPDP Act covers All digital personal data, including government & foreign entities.[40] The concept of consent has been upgraded now Explicit, informed, purpose-specific consent earlier in Often implied via privacy policies. Individual Rights were limited to correction via policy now it became the wider by allowing right to edit data, the right to be forgotten, the right to complain against the fiduciary of a grievance and even the right to nominate someone act on their behalf in case of their death or incapacity.[41]

For the enforcement**,** the IT Act relied on general tribunals (ad hoc tribunals) and low fines Max ₹25,000; the DPDP Act establish a specialized Data Protection Board and allows fines up to ₹250 crores.[42] The DPDP Act extends the scope and include extra-territorially (covering foreign entities that offer goods/services to Indians or monitor their behaviour), whereas the IT Act's privacy rules applied only to Indian corporates.

Still one of the important gaps is that in IT Act Section 43A /SPDI Rules where an individual can claim compensation for the failure to protect their data. The DPDP Act, 2023 does not provide a compensation for the breach of individual privacy. In fact, it expressly omits any remedy like Section 43A's damages[43]

8. COMPARATIVE LEGAL PERSPECTIVES

India has been considered to be experimenting with digital governance and these experiments have especially been compared with other global strategies such as that of Estonia, European Union and Singapore. Such comparisons bring light to the success of India as well as the negative areas.

8.1 Estonia:

The Pioneer of E-Governance Estonia is commonly known as the most digitalised society. Established digital identity and online voting as well as blockchain-based data registries are all part of Estonia governance since the 1990s[44]. The services are available, and can be accessed

[40] *DPDP Act vs. IT Act – Shifting India's Data-Protection Paradigm,* TAXMANN (May 4, 2025), https://www.taxmann.com (last visited Aug. 18, 2025)
[41] Press Release, Press Information Bureau, Gov't of India, Salient Features of the Digital Personal Data Protection Bill, 2023 (Aug. 9, 2023), https://pib.gov.in (last visited Aug. 18, 2025).
[42] *DPDP Act vs. IT Act – Shifting India's Data-Protection Paradigm,* TAXMANN, https://www.taxmann.com (last updated May 4, 2025).
[43] Bharat Manwani & Abhiraj Rana, *The Right to (Pry)-vacy: Understanding India's Dystopian Data Protection Legislation,* JILP BLOG (Feb. 12, 2024), https://jilpblog.com (last visited Aug. 18, 2025).
[44] *E-Governance in Estonia,* GOV'T OF ESTONIA, https://e-estonia.com (last visited Aug. 18, 2025).

by citizens via the X-Road platform, which is a secure data exchange layer in which e-services that were not originally related to each other can be offered. The exceptional thing about Estonia is that the country has a good legal framework, clear data-sharing standards and the citizens have trust in it. India has not made it to the level of the seamless integration and the level of protection of data under the same level that Estonia has. Estonia is an example that shows how administrative efficiency can be maximised under conditions of legal certainty, technological infrastructure and trust.

8.2 The European Union:

GDPR and Rights-Based Regulation General Data Protection Regulation of the European Union is the current high standard of data protection worldwide. Introducing concise principles of consent, purpose limitation, and data minimisation, GDPR introduces a right approach to governance[45]. The DPDP Act, 2023 of India is very much influenced by GDPR in taking its cue on consent and individual rights. India's Act also enables more exemptions to the government, which is a risk to the balance between efficiency and rights. The EU is an example of how rights-based regulation can allow innovation combined with transparency.

8.3 Singapore:

Smart Nation Strategy Singapore is a pragmatic smart nation that is integrating big data analytics, AI and IoT into its governance. The key capabilities are digital identity (SingPass), digital payments, and AI-based predictive tools of governance.[46] Unlike India, Singapore's smaller scale allows rapid implementation. The strategic capacity of the state, however, is an important part of its model. In India, Singapore is an example of how even in a rights-conscious regime, efficiencies of governance can be increased by introducing an agile policymaking model.

[45] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), 2016 O.J. (L 119) 1.
[46] *Smart Nation Singapore,* SMART NATION SINGAPORE, https://www.smartnation.gov.sg (last visited Aug. 18, 2025).

9. DIGITAL GOVERNANCE AND VIKSIT BHARAT 2047

Government of India vision on Viksit Bharat 2047 is a roadmap to achieving a developed economy in India on the 100th anniversary of Independence in 2047. Digital governance is recognized as one of the primary pillars of this Viksit Bharat 2047.

9.1 Goals of Viksit Bharat 2047

The strategy document focuses on citizen centric services, paperless government and governance by AI. It predicts universal connectivity and powerful data protection policies, and world supremacy in digital public infrastructure [47]

9.2 Administrative Efficiency as the Core Metric

By 2047, efficiency will no longer be gauged by considering only cost or speed, but also inclusivity, transparency and resilience. An example is that, grievance redress mechanisms should not only be fast to fix problems, but able to monitor systematic failures, and halt repeat.

The requirements of digital governance in sync with Viksit Bharat 2047 will thus have to focus on:

- Collegiality between systems within each department.
- Minimising human discrimination to limit corruption.
- Poise within the cyberattacks
- Bridge the gap with increased digital literacy.

9.3 Anticipated Legal Reforms

It is anticipated that the Digital India Act will replace IT Act, 2000, and look into AI, blockchain, and cross-border data governance issues with a modern framework decreased amount of money.[48] This law combined together with DPDP Act is likely to set the Indian digital governance course in the next 25 years.

[47] NITI AAYOG, GOV'T OF INDIA, VISION INDIA@2047: STRATEGY DOCUMENT (2022), https://www.niti.gov.in (last visited Aug. 18, 2025)
[48] Rajeev Chandrasekhar, Minister of State for Elecs. & Info. Tech., *Press Briefing on Draft Digital India Act* (Mar. 9, 2023), https://www.meity.gov.in (last visited Aug. 18, 2025).

10. LACK OF ALGORITHMIC ACCOUNTABILITY IN DIGITAL GOVERNANCE.

The framers of the Indian Constitution could barely have envisioned the digital age in which the work of government is performed not only by human officers, but through the use of algorithms and artificial intelligence (AI). The Constitution has proven to be quite elastic over the years but its true question is whether Information Technology Act of 2000 was formulated to deal with cybercrimes and digital transactions or constitutional dilemma of an algorithm-driven action. In the present, where India is aiming to make a Viksit Bharat by 2047, lack of constitutional checks by which digital governance mechanisms are controlled is a major issue.

10.1 Algorithms Without Adequate Oversight

The state is progressively using autonomous systems in the areas like welfare allocation, medicine and healthcare, policing and surveillance. These systems speed up the process but they also become a nightmare when the citizens remain deprived of benefits or become to be watched without any clear explanation. Such an error as an incompatible biometric data might deny the family food subsidies, and the dispensing of such a decision may not be explainable since the workings of the system are a black box. Such cases indicate that there is a governance gap in which the rights of citizens get denied if there is no accountable authority and no review mechanism in place.

10.2 Centrality of Article 21

Article 21 prevents that anyone shall be deprived of his or her life or personal liberty without following a procedure as prescribed by law. Courts have over the years given this meaning over time to include fairness, dignity and privacy (Maneka Gandhi, Puttaswamy). But when algorithmic-based procedures are opaque or may not be fair, Article 21 safeguarding becomes watered down. Automatic rejection of vital services becomes unappreciable due process and even becomes an unquestionable digital bureaucracy.

10.3 Global Experiences and India’s Lag

Accountability has begun being entrenched in the digital legislations of other jurisdictions. Both the European Union GDPR and Brazilian LGPD provide a person the right to seek an explanation of an automated decision. In comparison, India is stuck in the IT Act 2000 that

does not offer the algorithmic governance a constitutional prism. The constitutional safeguards need to become part of the negotiations in a new Digital India Act to ensure that the government is not absolving of responsibility and transferring accountability to non-human systems.

11. RECOMMENDATIONS

1. Make the Digital India Act by amending the IT Act into a legislation that brings contemporary technological facts on the grounds, such as AI and data flow across borders.

2. Enhance Data Protection while also reducing the number of exceptions to the DPDP Act so as to foster citizen confidence.

3. Close the Digital Divide and invest on broadband services and digital literacy schemes in the rural areas to bridge the digital divide, which will result in inclusive governance.

4. Institutionalise Cybersecurity with establishment of cyber to ensure security of critical infrastructure.

5. Increase Administrative Caliber by integrating future-oriented government processes (AI, data analytics) to be proactively inclusive in policymaking as opposed to reactively address grievances.

6. Global Harmonisation, aligning the data governance in India to ensure that it is with par as the international standards which in the end is able to transact with cross-border organizations with a sense of trust and assurance.

7. Furthermore, to bridge the gap and ensure digital governance to strengthens rather than weakens democracy, the following safeguards are vital:

- Reviewability: The deployed algorithms in the government should be subject to judicial review.
- Explainability: Automated decisions that impact rights have to be supplemented with clear, human understandable explanations.
- Transparency: The state should not hide the nature of AI tools use and location.
- Fairness: People should be able to appeal against the discriminative outcomes of algorithms.

12. CONCLUSION

The digital government in India has had successes and challenges. The Information Technology Act, 2000 was initially the legal monument that initiated electronic governance but ironically, with the passage of time its drawbacks came to the forefront. The changing interpretations of Judges, judicial landmark cases like Aadhaar, JAM Trinity, and CPGRAMS, as well as legislation reform like the DPDP Act, 2023, all point to the fact that India has headed towards speedier, transparent, and citizen-focused governance. Simultaneously, concerns related to privacy, legal frameworks that have not changed with the times, threats of cybersecurity breaches and the digital divide serve as reminders that technology does not merely ensure good governance in itself. Digital governance will form one of the most powerful columns of development as India looks forward to Viksit Bharat 2047. This vision will only be achieved if efficiency is mixed with accountability, and innovation is complemented with an inclusivity and trust. The proposed Digital India Act and other modifications have to be improved upon not only by updating the law, but also in the form of enhanced democratic protections such as privacy, openness, and fairness. The digital future of India must be quick as well as right, inclusive as well as intelligent, not only reachable but also citizen-friendly.

The Constitution will have to be updated to meet the challenges of algorithmic rule. The IT Act 2000 was a footstep towards digitalisation in India that needs to be integrated as the Constitution mandates in terms of accountability, fairness, and transparency in cyber systems in the journey towards Viksit Bharat 2047. Incorporation of algorithmic accountability into Article 21 will not only hinder the fundamental rights in the wake of technology but enhance the rule of law in the digital era.

“The future of governance is not simply e- governance, but responsible governance.”