The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2025

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

LEGAL ASPECTS OF CLOUD COMPUTING IN INDIA: BRIDGING INNOVATION AND REGULATION

-SAINATH GANDOLKAR

1. INTRODUCTION

Cloud computing provides on-demand, scalable access to computing resources via the Internet. According to the U.S. National Institute of Standards and Technology (NIST), it is a model for "ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources."[i] In India, the growing use of cloud-based services aligns with its digital economy ambitions, which are projected to expand from $200 billion to $1 trillion by 2025.[ii] Initiatives like Digital India and *Make in India* promote this shift. However, hosting vast data on third-party servers presents privacy and security risks, especially if providers falter in compliance.[iii] Hence, the legal dimensions of cloud computing—covering data protection, liability, and jurisdiction—are gaining attention.

2. PROVISIONS UNDER THE ACTS AND CONVENTIONS

India lacks a dedicated law for cloud computing. Relevant provisions are mainly embedded in general statutes, particularly the **Information Technology Act, 2000**, as amended in 2008. The Act facilitates a secure environment for digital transactions and penalizes various cyber offenses.[iv] Under §43, unauthorized access to systems or data—such as downloading or altering without consent—is actionable.[v] Sections 65 and 66 penalize tampering and hacking, while §72 sanctions breaches of data confidentiality.[vi] These apply whether data resides on a local server or a cloud platform. Additionally, the 2011 SPDI Rules require privacy policies, consent, and reasonable security from data handlers.[vii] Noncompliance under §43A permits compensation for data breaches.[viii]

Cloud contracts, governed by the **Indian Contract Act, 1872**, typically take electronic form. Validity hinges on standard principles like offer and acceptance. The IT Amendment Act of 2008 clarified through §10A that e-contracts carry legal validity.[ix] Courts uphold these, including user-agreed service terms like disclaimers or arbitration clauses.

For dispute resolution, the **Arbitration and Conciliation Act, 1996**, aligned with UNCITRAL standards, facilitates cross-border arbitration. India's status as a party to the 1958 New York Convention reinforces this.[x] Yet, it has not joined the **Budapest Convention on Cybercrime**, hindering cooperation in international cyber investigations.[xi] Assistance is instead rendered via bilateral or mutual legal arrangements. Additional laws like the Indian Telegraph Act of 1885 or the Wireless Telegraphy Act of 1933 permit government interception of cloud communications, though these are sparingly applied.

3. LEGAL ISSUES IN CLOUD COMPUTING

i. Privacy

In 2017, the Supreme Court declared privacy a fundamental right under Article 21.[xii] Historically, privacy was governed through fragmented rules like SPDI. The 2023 **Digital Personal Data Protection (DPDP) Act** marked a shift by requiring consent or legitimate purpose for data use, breach notifications, and user rights like correction and access.[xiii] It mirrors GDPR's principles and authorizes conditional cross-border data flows. Though less stringent than earlier drafts, the DPDP Act is a significant privacy milestone. SPDI Rules and IT Act §43A remain relevant for corporate liability.[xiv]

ii. Security

Cloud security is a shared responsibility: providers secure the infrastructure, while users safeguard applications and data keys. When breaches occur, users often seek remedies under §43A (security failures) or §72 (unauthorized disclosure). For example, if cloud misconfiguration by a bank causes data theft, the bank may be liable.[xv] Cloud service contracts usually limit provider liability, and user negotiation power is minimal. Legal consensus is unclear on provider accountability for knowingly hosting unlawful content.[xvi]

iii. Jurisdiction and Data Sovereignty

Cloud storage often spans multiple jurisdictions. Contracts specify applicable law and forum; Indian courts accept these when reasonable.[xvii] However, foreign jurisdiction clauses (like U.S. or Singapore) often disadvantage Indian consumers. India currently does not enforce strict data localization, unlike GDPR-compliant EU states or Russia. The DPDP Act restricts some data transfers and allows regulatory intervention, but does not mandate localization. Consequently, remedies for Indian users against foreign providers remain limited.[xviii]

iv. Other Issues

Standard-form contracts limit user negotiation, typically enforcing broad licenses and arbitration clauses.[xix] Lack of interoperability also raises concerns; proprietary systems hinder data portability and create vendor lock-in.[xx] Moreover, Indian regulators (e.g., SEBI, TRAI) have yet to release tailored cloud-specific rules, though stakeholders demand guidance on security benchmarks and consumer safeguards.

4. GOVERNMENT INITIATIVES AND MARKET TRENDS

The government's commitment is evident through projects like **GI Cloud (Meghraj)**, initiated in 2015. Meghraj provides a federated cloud for central and state agencies. The aim is efficient public service delivery and cost reduction via infrastructure sharing. Additionally, the 2022–23 Union Budget recognized data centers as infrastructure, qualifying them for incentives.[xxi] Prime Minister Modi has envisioned India as a "global data center hub."[xxii] To this end, the **Draft Data Centre Policy (2020)** promotes investment, sovereignty, and standardized frameworks.[xxiii]

Market-wise, the Indian cloud sector is rapidly expanding. Public cloud services are forecasted to reach $17.8 billion by 2027.[xxiv] Global players like Amazon, Microsoft, and Google have established Indian data regions, meeting regulatory and performance needs. Domestic IT firms like TCS and Infosys have also ventured into cloud services. Netmagic (under NTT Data) runs several Indian data centers.[xxv] Demand is rising across sectors—particularly fintech, education, and startups—as cloud adoption accelerates.

5. CONCLUSION

Cloud computing offers transformative potential for India. But its success hinges on legal readiness. Currently, a mix of the IT Act, contract law, and sectoral policies govern cloud usage. While the new DPDP Act and cloud-related initiatives mark progress, ambiguities persist around localization, security standards, and fairness in service terms.[20] As India further digitizes, evolving legal clarity will be essential for balancing innovation with accountability.

ENDNOTES

[i] U.S. Nat'l Inst. of Standards & Tech., *NIST Special Publication 800-145*, at 2, 4 (2011)

[ii] Ministry of Electronics & IT, Govt. of India, *India to be a Cloud Computing and Data Centre Hub* 1–2 (Dec. 8, 2022), https://pib.gov.in (Press Release).

[iii] ibid

[iv] G.A. Solanki, *Welcome to the Future of Computing: Cloud Computing and Legal Issues*, 1 Int'l J. of Adv. Research 61, 65–66 (2012)

[v] Information Technology Act, 2000, No. 21, Acts of Parliament, 2000, § 43

[vi] Information Technology Act, 2000, No. 21, Acts of Parliament, 2000, §§ 65, 66, 72 (India)

[vii] Information Technology (SPDI) Rules, 2011, G.S.R. 313(E) (Apr. 11, 2011) (India).

[viii] Ibid

[ix] Gowri Menon, *Regulatory Issues in Cloud Computing – An Indian Perspective*, 2 Int'l J. of Electronic Com. 85, 86–87 (2013).

[x] Divyaraj Ray, *Cloud Computing and Challenges Faced in Existing Legal Structure*, 2 Jus Corpus L.J. 257, 259–60 (2021).

[xi] D.P. Tiwari, *Cloud Computing: Liability and Legal Issues in India*, 7 J. of Tech. L. 488, 490–92 (2021).

[xii] Justice K.S. Puttaswamy (Retd.) & Ors. v. Union of India, (2017) 10 SCC 1 (India).

[xiii] National Informatics Centre, *National Cloud (Meghraj)*, available at https://www.nic.gov.in/service/national-cloud (accessed July 2025).

[xiv] Divyaraj Ray, *Cloud Computing and Challenges Faced in Existing Legal Structure*, 2 Jus Corpus L.J. 257, 259–60 (2021).

[xv] Gowri Menon, *Regulatory Issues in Cloud Computing – An Indian Perspective*, 2 Int'l J. of Electronic Com. 85, 86–87 (2013).

[xvi] Nishith Desai Assocs., *Cloud Computing: Risks/Challenges – Legal & Tax Issues* 10–11 (2013), http://www.nishithdesai.com.

[xvii] Pritish Sahoo & Taruna Jaiswal, *Cloud Computing and Its Legalities in India*, 4 Nirma Univ. L.J. 65, 68–70 (2014).

[xviii] Anirudh Burman, *Understanding India's New Data Protection Law* 1–3 (Carnegie Endowment, Oct. 3, 2023).

[xix] G.A. Solanki, *Welcome to the Future of Computing: Cloud Computing and Legal Issues*, 1 Int'l J. of Adv. Research 61, 65–66 (2012).

[xx] ibid

[xxi] Ministry of Finance (India), *Budget 2022–23 Speech*, at 10–11 (Feb. 1, 2022).

[xxii] Prime Minister Narendra Modi, *Address at Launch of Microsoft Hyderabad Data Centre* (Nov. 21, 2022), https://pib.gov.in (see "Make India a data centre hub" statement).

[xxiii] Ministry of Electronics & IT (India), *Data Centre Policy: Draft* 2020, at 1–2 (2020).

[xxiv] Nirmal Bang Institutional Equities, *India IT Sector Thematic Report*, at 26 (Sept. 4, 2024). (Projecting India's public cloud market at US$17.8 billion by 2027.)

[xxv] CloudScene, *Global Data Centres by Country* (Jan. 2021), cited in SCC Online (India) news report.