*Page 450 - 457* **DOI:** *https://doij.org/10.10000/IJLMH.119728*

# INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

**Volume 8 | Issue 3**

**2025**

© 2025 *International Journal of Law Management & Humanities*

Follow this and additional works at: https://www.ijlmh.com/
Under the aegis of VidhiAagaz – Inking Your Brain (https://www.vidhiaagaz.com/)

This article is brought to you for "free" and "open access" by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of **any suggestions or complaints**, kindly contact **support@vidhiaagaz.com**.

**To submit your Manuscript** for Publication in the **International Journal of Law Management & Humanities**, kindly email your Manuscript to **submission@ijlmh.com.**

# Contemporary Challenges to Privacy in the Digital Era Legal and Judicial Responses

CHETAN DALAL[1] AND HIMANSHU VARSHNAY[2]

## ABSTRACT

*In the digital era, the right to privacy faces multifaceted challenges arising from rapid technological advancements, state surveillance, and inadequate regulatory frameworks. This dissertation critically examines how emerging technologies—such as facial recognition, the Internet of Things (IoT), artificial intelligence (AI), and big data analytics—pose significant risks to individual privacy in India. It analyzes the legal responses, including the enactment of the Digital Personal Data Protection Act, 2023 (DPDPA), and the evolving jurisprudence shaped by landmark judgments. The study highlights the gaps in implementation, the lack of algorithmic transparency, and the broad exemptions granted to government agencies. It further conducts a comparative analysis between India's DPDPA and the European Union's GDPR, drawing insights from global best practices. By assessing sectoral regulations, recent case law, and institutional developments, the research underscores the urgent need for robust enforcement mechanisms, ethical oversight, digital literacy, and a privacy-first design philosophy. The dissertation concludes that balancing technological innovation, economic interests, and national security with the constitutional right to privacy is the defining challenge for India's digital future.*

## I. EMERGING TECHNOLOGIES AND NEW FRONTIERS OF PRIVACY RISK

### Facial Recognition and Internet of Things (IoT)

The rapid growth of facial recognition technology and the extensive use of Internet of Things (IoT) devices have created intricate privacy challenges in India. Increasingly utilized for public surveillance, airports, and law enforcement, facial recognition systems can monitor and identify people without their permission, raising profound worries about mass surveillance and the diminishing of anonymity in public areas. The insufficient regulatory framework leaves minimal protections against the mishandling of biometric information, possible profiling, and inaccurate identifications. The use of such technology by both government and private entities, often lacking transparent policies or effective avenues for redress, has heightened demands for more stringent legal criteria and independent regulatory bodies.

[1] Author is a Student at Amity University Noida, India.
[2] Author is an Assistant Professor at Amity University Noida, India.

© 2025. International Journal of Law Management & Humanities [ISSN 2581-5369]

Similarly, IoT devices—ranging from smart home assistants to wearable health monitors—continuously gather, transmit, and occasionally share sensitive personal information. Numerous devices hail from foreign manufacturers, with data stored on servers situated outside of India, complicating the enforcement of Indian privacy legislation. The lack of strong encryption measures, regular software vulnerabilities, and insufficient user knowledge further intensify the risks of unauthorized access, hacking, and data breaches. The government's initiative for data localization partly responds to these issues, aiming to guarantee that the data of Indian citizens remains within the nation and is governed by local legal safeguards.

### Artificial Intelligence, Big Data, and Algorithmic Bias

Artificial intelligence (AI) and big data analytics have become essential components in sectors such as healthcare, finance, and governance in India. AI systems analyze vast amounts of personal information to offer tailored services and automate decision-making. Nevertheless, these technologies can also sustain algorithmic bias, discriminate against marginalized communities, and produce opaque decisions that are challenging to contest. For instance, AI-generated credit scoring or predictive policing could exacerbate existing societal biases if trained on flawed datasets, resulting in unjust outcomes for individuals.

India's legal framework is still in the process of adapting to these advances. The Digital Personal Data Protection Act, 2023 (DPDPA), along with its draft regulations, seeks to tackle some of these hazards by requiring transparency, accountability, and regular audits for significant data fiduciaries—entities managing large quantities or sensitive types of data. However, the absence of clear provisions regarding algorithmic explainability and the right to dispute automated decisions represents a significant gap. As AI continues to grow in prevalence, there is an urgent need for sector-specific policies, ethical standards, and regulatory sandboxes to ensure that technological progress does not compromise individual rights and dignity.

## II. Recent Legal and Regulatory Developments

### The Digital Personal Data Protection Act, 2023 and Draft Rules, 2025

The enactment of the DPDPA in August 2023 signified a significant milestone in India's privacy legislation. The Act establishes a consent-focused framework that mandates explicit, informed, and revocable consent for personal data processing. It confers rights upon individuals (data principals) such as access, amendment, deletion, and grievance resolution, while imposing stringent responsibilities on data fiduciaries (organizations managing personal data).

The Draft Digital Personal Data Protection Rules, 2025, which were made available for public

feedback in January 2025, are set to implement the DPDPA. Noteworthy aspects include:

- Children's Data Privacy: Platforms are required to obtain verifiable parental consent prior to processing minors' data, with parental identification verified through government-recognized documents or digital platforms like DigiLocker. This aims to safeguard younger individuals from exploitation and ensure accountability.
- Data Retention and Deletion: Personal data may only be retained as long as needed for its designated purpose and must be deleted afterward, in accordance with global principles of data minimization.
- Consent Managers: The guidelines introduce consent managers as intermediaries to assist individuals in granting, managing, or revoking their consent, providing users with enhanced control over their personal information.
- Mandatory Security Protocols: Data fiduciaries are obligated to enforce robust security practices, including encryption and real-time surveillance, to avert breaches.
- Uniform Data Breach Reporting: Fiduciaries must inform both the Data Protection Board and affected individuals of any breaches, thus enhancing transparency and accountability.
- Cross-Border Data Localization: The draft guidelines place restrictions on cross-border data transfers, necessitating explicit government authorization, which bolsters data sovereignty but may pose compliance challenges for international firms.
- Significant Data Fiduciaries (SDFs): Organizations managing substantial volumes or sensitive types of data must perform annual audits and impact assessments to maintain compliance.

These regulations are anticipated to transform India's digital landscape while balancing innovation with strong privacy safeguards. Nevertheless, operational difficulties, such as ensuring compliance across various sectors and addressing high compliance costs for smaller businesses, continue to be considerable challenges.

**Sectoral Regulatory Initiatives**

Beyond the DPDPA, sectoral regulators are increasingly taking initiative. The Insurance Regulatory and Development Authority (IRDAI), Securities and Exchange Board of India (SEBI), and Reserve Bank of India (RBI) have all released guidelines demanding that regulated entities adopt enhanced security measures for data storage, privacy, and confidentiality, particularly in cloud computing and fintech. These specialized measures work alongside the

© 2025. International Journal of Law Management & Humanities [ISSN 2581-5369]

DPDPA and demonstrate a broader governmental commitment to prepare the country for emerging sector-specific privacy challenges.

### Recent Case Law and Judicial Trends

Indian courts have maintained a crucial role in interpreting and upholding privacy rights. In R v. B (SCC OnLine Mad 6084, 2024), the Madras High Court ruled that acquiring and presenting a spouse's call data records without their consent was a clear violation of spousal privacy and therefore inadmissible in court. The Court underscored that privacy as a fundamental right encompasses marital relationships and that evidence procured in violation of this right cannot be accepted in legal contexts.

Additionally, the Supreme Court's ongoing supervision in the WhatsApp-Facebook privacy policy litigation has ensured that users are not compelled to agree to unilateral policy modifications that jeopardize their privacy. The Competition Commission of India's fine imposed on Meta for "take-it-or-leave-it" consent showcases the increasing regulatory intolerance for coercive data practices.

## III. Persistent and Evolving Privacy Challenges

### State Surveillance and Overreach

India's surveillance systems, such as the Centralized Monitoring System (CMS) and extensive reliance on Section 69A of the IT Act (which permits government blocking of information for national security), have raised alarms about government overreach and the lack of independent oversight. The Pegasus spyware incident and ongoing discussions about lawful interception highlight the conflict between national security and personal privacy. Although the Supreme Court has called for procedural safeguards and judicial oversight, the absence of a thorough surveillance law and the wide-ranging exemptions provided to government bodies under the DPDPA continue to present issues.

### Data Breaches and Cybersecurity Threats

India has experienced multiple significant data breaches, including the exposure of Aadhaar data involving over 800 million people and recurrent cyberattacks targeting financial institutions and government databases. The DPDPA and its draft provisions now require immediate breach notifications and impose severe penalties for non-compliance. However, enforcing these regulations poses challenges due to limited regulatory resources and insufficient technical expertise. The demand for data localization is partly driven by the goal to improve cybersecurity and ensure that Indian data is protected under domestic laws, but it also raises

operational and cost concerns for businesses functioning on an international scale.

### Lack of Public Awareness and Digital Literacy

A major obstacle to effective privacy protection in India is the widespread lack of knowledge among citizens and businesses regarding their rights and responsibilities. Many users are oblivious to how their data is collected, managed, and shared, resulting in numerous violations and underreporting of breaches. The DPDPA and related regulations call for enhanced transparency and user empowerment, but these initiatives will be effective only if paired with ongoing public education campaigns and digital literacy programs.

### Cross-Border Data Flows and Jurisdictional Complexities

The global character of the internet means that data belonging to Indian users is frequently stored and processed on servers located overseas, and thus subject to differing levels of protection under foreign laws. This creates obstacles for enforcement, especially when foreign companies fall outside Indian jurisdiction or when international law enforcement agencies (e.g., under the US CLOUD Act) require access to data housed in India. The DPDPA's limitations on cross-border data transfers and its focus on "trusted jurisdictions" aim to tackle these challenges, yet practical execution and international collaboration remain complex.

## IV. Comparative Analysis: India and Global Standards

### GDPR vs. DPDPA: Key Similarities and Differences

The DPDPA is inspired by the EU's General Data Protection Regulation (GDPR) but differs in various ways:

- Scope and Application: GDPR has a global reach, applying to any organization handling data of EU residents, while the DPDPA pertains to organizations dealing with data of Indian residents, including those outside India that provide goods or services to Indians.
- Individual Rights: Both frameworks offer rights such as access, correction, erasure, and objection to processing, but GDPR provides broader rights, such as data portability and the right to contest automated decision-making.
- Enforcement and Penalties: GDPR imposes fines up to 4% of global revenue or €20 million, whichever is higher. The DPDPA enforces penalties up to ₹500 crore, and the Data Protection Board of India has the authority to mandate urgent remedial actions.
- Cross-Border Transfers: GDPR has more stringent requirements for international data transfers, necessitating "adequate protection" in receiving countries. In contrast, the

DPDPA restricts transfers and mandates explicit governmental approval, emphasizing data sovereignty.

- Government Exemptions: The DPDPA grants broader exemptions to governmental agencies, raising concerns about uncontrolled state surveillance.
- Implementation and Enforcement: GDPR has established independent supervisory bodies and a strong enforcement framework, whereas the operationalization of DPDPA's Data Protection Board is still in progress and grapples with capacity challenges.

### Insights from Global Practices

India can draw lessons from the GDPR's focus on independent oversight, robust enforcement, and clearly defined rights for data subjects. The GDPR mandates organizations to document their data processing activities, perform impact assessments, and set up mechanisms for addressing grievances, which could guide future revisions of the DPDPA. The US's sectoral approach (such as CCPA and HIPAA) illustrates the benefits of customizing privacy protections for specific industries while also revealing the dangers of inconsistent standards.

## V. RECOMMENDATIONS AND THE PATH FORWARD

### Enhancing Implementation and Enforcement

- Capacity Development: The Data Protection Board and sector-specific regulators require sufficient funding, expertise, and autonomy to effectively enforce privacy legislation.
- Routine Audits and Impact Evaluations: Imposing mandatory audits for significant data fiduciaries and conducting regular privacy impact assessments can aid in proactively identifying and managing risks.
- Protections for Whistleblowers: Legal safeguards for those who report data misuse or violations within organizations can bolster accountability and promote a culture of compliance.

### Promoting Public Awareness and Digital Literacy

- Public Education Initiatives: Nationwide efforts to inform citizens about their privacy rights, the dangers of data sharing, and available redress mechanisms are crucial for empowering users meaningfully.

© 2025. International Journal of Law Management & Humanities [ISSN 2581-5369]

- Digital Literacy Initiatives: Incorporating privacy and cybersecurity education into the curricula at schools and universities will contribute to building a society aware of privacy issues.

**Policy and Technological Advancement**

- Privacy by Design: Integrating privacy principles into the development of digital products and services should be standard practice rather than an afterthought.
- Ethical AI and Accountability in Algorithms: Establishing sector-specific conduct guidelines for AI, necessitating transparency, and creating mechanisms for addressing algorithmic harms are vital for responsible innovation.
- Global Collaboration: India should engage actively in global discussions to align privacy standards, facilitate cross-border data flows, and tackle jurisdictional challenges.

**Tackling Emerging Threats**

- Regulation of Facial Recognition and Biometric Surveillance: Clear legal frameworks for the application of facial recognition and biometric data must be formulated, including requirements for transparency, consent, and independent oversight.
- Protecting IoT Ecosystems: Strong security measures and periodic vulnerability assessments for IoT devices should be mandated, and manufacturers must provide transparent privacy policies and user controls.
- Preventing Data Breaches: Stricter requirements for breach notifications should be implemented, alongside promoting encryption and increasing penalties for careless data management.

## VI. CONCLUSION

The digital evolution of Indian society has yielded significant advantages but also brought unprecedented privacy challenges. As India puts the DPDPA into practice and sectoral regulators increase their vigilance, the emphasis should transition from simple compliance to cultivating a digital culture that respects privacy. Achieving this necessitates not just strong laws and independent oversight but also technological advancements, public education, and international cooperation. As emerging technologies like AI, facial recognition, and IoT alter the privacy landscape, India's legal and policy frameworks must remain flexible, responsive, and grounded in the constitutional principles of dignity, autonomy, and personal freedom. The

ultimate challenge will be India's ability to balance innovation, economic development, and national security with the fundamental right to privacy, a challenge that will shape the future of its digital democracy.

*****

© 2025. International Journal of Law Management & Humanities [ISSN 2581-5369]