Data Privacy, AI and Technology Updates: October 2025–January 2026 – Newsletter

Introduction

India is currently experiencing a period of unprecedented digital transformation, driven by rapid advancements in Artificial Intelligence ("**AI**") and a parallel effort to develop a robust legal framework for data governance. This transformation places India at the forefront of global policy discourse on balancing technological growth with the protection of the fundamental right to privacy for its 1.42 billion citizens.

This widespread adoption of AI across sectors such as public services, finance, healthcare and national security has significantly altered how data is generated, processed and consumed. In this context, India's evolving regulatory framework has drawn significant national and international interest.

The operationalization of the Digital Personal Data Protection Act, 2023 ("**DPDP Act**"), marks a major step in India's approach to personal data. The DPDP Act establishes a consent-based framework for data processing in India, imposes obligations for Data Fiduciaries and empowers Data Principals with rights such as erasure and grievance redressal. It also permits cross-border data transfers subject to restrictions notified by the Central Government, enabling international business while retaining regulatory oversight. With the notification of the Digital Personal Data Protection Rules, 2025 ("**DPDP Rules**"), these principles have now been translated into practical compliance requirements. The DPDP Rules explain how consent and notices must be presented, recognise Consent Managers, and place additional responsibilities on Significant Data Fiduciaries. They also introduce safeguards for children's data and outline the powers of the Data Protection Board of India.

This period has seen significant regulatory activity across areas such as telecom cybersecurity, digital payment authentication, dark patterns, cybercrime enforcement, consumer protection, and the use of technology in the justice system. Authorities and courts have responded to emerging risks involving AI-generated content, cyber fraud, data misuse, and misleading online design practices. At the same time, new technological

measures, from AI-assisted law enforcement tools to stronger UPI authentication, reflect efforts to build a more secure and responsible digital environment. These developments show how quickly India's digital framework is evolving and the importance of staying alert to shifting regulatory expectations.

OCTOBER

Telecommunications (Telecom Cyber Security) Amendment Rules, 2025

The Telecommunications (Telecom Cyber Security) Amendment Rules, 2025 ("**2025 Amendment Rules**"), issued under the Telecommunication Act, 2023, modify and expand the earlier Telecommunications (Telecom Cyber Security) Rules, 2024 ("**2024 Rules**"). The amendments introduce Mobile Number Validation ("**MNV**"), under which the Central Government or its designated agency must establish and operate a secure validation platform to authenticate telecom identifiers such as mobile numbers and IMEIs. Telecom Service Providers ("**TSPs**") and other authorized entities are mandated to participate in this platform by responding to, processing, and validating requests made by approved users.

The Department of Telecommunications ("**DoT**"), acting as the administrative department for implementing the Rules, has the authority to direct Telecom Identifier User Entities ("**TIUEs**"), including digital platforms, fintech companies, retailers, etc., to use the MNV platform. These entities rely on mobile numbers for verification or communication. TIUEs must verify that a number is registered to the claimed user in a telecom operator's database before relying on it for their services. TIUEs are also required to submit details to the DoT concerning their usage of telecom identifiers. They must adhere to government-mandated cybersecurity directions issued under the 2024 Rules and the 2025 Amendment Rules. The DoT is also empowered to direct TSPs and TIUEs to block or suspend a telecom identifier in the public interest if misuse is identified. Such directions may be issued without prior notice. However, the reasons for issuing them must be recorded in writing.

Proposed amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, in relation to synthetically generated information

The Ministry of Electronics and Information Technology ("**MeitY**") has proposed amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ("**IT Rules**") to regulate synthetically generated content, including deepfakes, misinformation, and digitally manipulated media.

The amendments propose a statutory definition of synthetically generated information and clarify its scope under Rules 3(1)(b)&(d) and Rules 4(2)&(4) of the IT Rules. Intermediaries, especially Significant Social Media Intermediaries, are required to label synthetic or altered content, embed permanent unique metadata identifying manipulated information, and deploy technical tools to detect and flag deepfakes. The proposal seeks to balance intermediaries' liability protection under Section 79(2) of the Information Technology Act, 2000 ("**IT Act")**, while addressing user grievances related to deepfakes or synthetic content.

Central Goods and Services Tax (Fourth Amendment) Rules, 2025

The Central Board of Indirect Taxes and Customs has notified the Central Goods and Services Tax (Fourth Amendment) Rules, 2025, which amend the Central Goods and Services Tax Rules, 2017. These changes introduce a fast-track and data-driven process for GST registration for taxpayers with lower monthly output tax liabilities. The amendments were notified on 31 October 2025 and came into effect on 1 November 2025.

The amendment inserted two new rules, i.e., Rule 9A and Rule 14A, introducing a simplified registration process for eligible taxpayers. Rule 9A establishes a fully digital, fast-track registration mechanism enabling automatic grant of electronic registrations within three working days for specified applicants falling under Rules 8, 12 and 17. Rule 14A introduces an optional registration scheme for taxpayers whose monthly total tax liability does not exceed Rs. 2,50,000, subject to specified conditions, including Aadhaar

authentication, single registration per state/union territory, and grant of electronic registration within three working days.

NPCI introduces On-Device biometric authentication for UPI

The National Payments Corporation of India ("**NPCI**"), through its operational circular dated 7 October 2025, has authorized additional authentication methods for Unified Payments Interface ("**UPI**") transactions. Payment systems participants have been permitted to implement authentication using a device's native biometric sensors, such as fingerprint scanners and facial recognition systems, as well as FIDO-based passkeys, to authenticate UPI payments.

By reducing dependence on static PIN-based mechanisms, the framework enhances protection against unauthorized access and strengthens digital payment security. The implementation is part of NPCI's roadmap for rolling out advanced authentication mechanisms across the UPI ecosystem during the latter part of 2025.

MeitY & CERT-In highlight National Cyber Security Awareness Month

October 2025 was observed as National Cyber Security Awareness Month, with the official theme "Cyber Jagrit Bharat" (Cyber Safe India). This theme reinforced the importance of collective responsibility in safeguarding India's digital ecosystem and highlighted the role of individuals, enterprises, and public institutions in strengthening cyber resilience.

The Indian Computer Emergency Response Team ("**CERT-In**") has been designated to serve as the national agency for incident response under Section 70B of the IT Act. As part of the awareness initiative, CERT-In focused on the adoption of multi-factor authentication across banking, email, and social media accounts to reduce compromise risks; awareness of evolving cyber threats, including phishing, smishing, and vishing attacks, particularly those using generative AI; cautious digital behaviour, including detection of suspicious links and attachments; and timely reporting of incidents to the appropriate authorities.

NOVEMBER

Government notifies Digital Personal Data Protection Rules, 2025

The Government notified the DPDP Rules, giving full operational effect to the DPDP Act. The DPDP Rules establish practical obligations for Data Fiduciaries, including the detailed requirements for valid consent, notice and disclosure obligations, and grievance redressal procedures for Data Principals. The DPDP Rules also formally recognise Consent Managers as regulated entities responsible for enabling individuals to manage, grant, and withdraw consent.

The DPDP Rules introduce additional compliance obligations on Significant Data Fiduciaries, including mandatory Data Protection Impact Assessments, periodic audits by independent auditors, and the appointment of a Data Protection Officer. Separate provisions address the processing of children's data, including stricter consent requirements and prohibitions on tracking and targeted advertising. The DPDP Rules further prescribe standards for data breach reporting. They also specify timelines for notifying affected Data Principals. In addition, the DPDP Rules empower the Data Protection Board of India to issue directions, conduct inquiries, and impose penalties for non-compliance.

CERT-In Issues series of security advisories for November 2025

The CERT-In released a series of security advisories during November 2025, highlighting critical vulnerabilities in products and services from multiple technology vendors. The advisories include technical details such as Common Vulnerabilities and Exposures identifiers, severity ratings, and affected software versions. CERT-In has prescribed immediate application of vendor patches, adoption of interim mitigation measures where patches are unavailable, and strengthening of monitoring mechanisms to detect and address exploitation attempts.

CCPA secures compliance from major e-commerce platforms on dark patterns

The Central Consumer Protection Authority ("**CCPA**") confirmed that 26 leading e-commerce platforms submitted formal self-declarations between 20 and 24 November

2025, affirming compliance with its advisory against deceptive user-interface practices commonly described as "dark patterns."

The declarations confirm that platforms have aligned their design practices with regulatory guidance, including discontinuing techniques such as false urgency, basket sneaking, confirm shaming, and forced actions. This development reinforces the regulatory focus on transparency, consumer autonomy, and fair digital commerce practices.

TRAI initiates consultation on review of Interconnection Regulations

The Telecom Regulatory Authority of India issued a consultation paper on 10 November 2025, inviting stakeholder comments on a comprehensive review of its existing regulations governing interconnection. This exercise aims to reassess the current framework for network, spectrum, and licensing matters to ensure it remains relevant and effective in the context of evolving telecom technologies and market structures. The consultation paper seeks to examine the adequacy of present interconnection rules in fostering competitive markets and ensuring quality service for consumers.

RBI Updates Guidance on Digital Rupee (e₹) Pilot

The Reserve Bank of India updated its Frequently Asked Questions ("**FAQs**") on 20 November 2025 and issued revised guidance concerning the Central Bank Digital Currency, known as the Digital Rupee (e₹). This update provides crucial clarifications and reflects the evolving scope of the ongoing digital rupee pilot, serving as an authoritative source for financial institutions and the public on the project's status and operational mechanics.

The revised FAQs offer detailed insights into the objectives of the digital rupee, its operational framework, and the distinct features of both the retail and wholesale variants. It also addresses key areas of public interest, including the process for user onboarding and transactions, the underlying technology, and the measures implemented to ensure privacy and security.

DECEMBER

NCLAT upholds Rs. 213.14 crore penalty on Meta in WhatsApp privacy policy case[1]

The National Company Law Appellate Tribunal ("**NCLAT**") upheld the Rs. 213.14 crore penalty imposed by the Competition Commission of India ("**CCI**") on Meta Platforms for abusing its dominant position through WhatsApp's 2021 Privacy Policy update, which compelled users to accept expanded data collection and sharing within the Meta group on a "take-it-or-leave-it" basis.

While the NCLAT affirmed the CCI's jurisdiction to examine anti-competitive issues arising from data collection and upheld key remedies mandating transparency, purpose limitation, and meaningful user choice, including opt-out mechanisms, it set aside the findings under Section 4(2)(e) and paragraph 247.1 of the CCI order. This permits WhatsApp to share user data with Meta companies for advertising purposes ahead of the previously stipulated five-year restriction, partially addressing consumer harm but raising nuanced concerns that require deeper analysis.

MeitY reiterates due diligence obligations for VPNs and intermediaries

MeitY has issued an advisory reminding VPN service providers and intermediaries of their due diligence obligations under the IT Act and the IT Rules. The advisory highlights concerns over illegal websites such as proxyearth.org and leakdata.org that publicly disclose sensitive personal data of Indian users without authorisation, posing serious privacy and security risks.

MeitY has emphasised that intermediaries must ensure such unlawful content is neither hosted nor accessed, including through VPN services, and must act promptly to remove or block it. Failure to comply with due diligence obligations will result in loss of safe harbour protection under Section 79 of the IT Act, attracting liability and action under applicable laws, including the Bharatiya Nyaya Sanhita, 2023.

[1] Whatsapp LLC v. Competition Commission of India, 2025 SCC OnLine NCLAT 38.

The advisory further reiterates that intermediaries are legally bound to cooperate with authorised government agencies for investigation, verification, and cybersecurity purposes.

Supreme Court reconstitutes AI Committee to advance tech-enabled justice

Chief Justice of India Surya Kant has reconstituted the AI Committee of the Supreme Court, reaffirming the judiciary's commitment to technology-driven reforms. The committee will be chaired by Justice P. S. Narasimha and includes Chief Justice Sanjeev Sachdeva and Justices Raja Vijayaraghavan V, Anoop Chitkara, and Suraj Govindaraj from various High Courts. Anupam Patra, OSD (Technology), Supreme Court of India, will act as Secretary and Convenor, with Ashish J. Shiradhonkar of the eCommittee joining as a Special Invitee.

The reconstituted body will provide strategic oversight on the adoption and deployment of AI across the Supreme Court and subordinate judiciary. Its focus includes improving case management, scheduling, and documentation to reduce delays and enhance efficiency. The initiative also aims to strengthen accessibility and transparency, making judicial processes more user-friendly and accountable.

Supreme Court directs pan-India CBI probe into digital arrest scams[2]

The Supreme Court of India has directed the Central Bureau of Investigation ("**CBI**") to prioritise and lead a nationwide investigation into the digital arrest scams, a cyber-extortion racket targeting mainly senior citizens through impersonation of law enforcement and judicial authorities. The Court took *suo motu* cognisance of the issue after multiple FIRs emerged across states and noted the scale of financial losses linked to organised networks employing fake video calls, fabricated orders, and psychological coercion to demand money. In its order, the Court emphasised that digital arrest scams require the "immediate attention" of the investigating agency and directed that the CBI should take the lead in probing these cases before other categories of cyber fraud.

[2] In Re: Victims of Digital Arrest Related to Forged Documents, SNW (Crl.) 3/2025.

The Court authorised CBI to examine the role of bankers under the Prevention of Corruption Act, 1988, in cases involving "mule accounts" used to receive extorted funds. It empowered CBI to seek assistance from Interpol authorities where cross-border activity is uncovered. The Court also sought support from the Reserve Bank of India to explore the use of AI and machine-learning tools for detecting and freezing suspicious accounts. It directed state authorities and intermediaries under the IT Rules to cooperate with investigative efforts. Observing the disproportionate impact on elderly victims, the Court stressed a coordinated regulatory response extending beyond arrests, including improvements in telecom issuance norms and state cybercrime infrastructure.

Kerala High Court flags unchecked use of AI in drafting writ petitions[3]

The Kerala High Court has cautioned against the growing reliance on AI tools by lawyers for drafting writ petitions without adequate legal research. The Court observed that several AI-generated petitions lack basic material facts, leaving advocates unable to answer judicial queries.

The Court noted a surge in petitions seeking the de-freezing of bank accounts amid rising cyber fraud cases, often filed by young lawyers with incomplete pleadings. Expressing concern over misuse of jurisdiction and forged filings, the Court directed that local SHOs be impleaded in such cases to prevent impersonation. The directions have, however, drawn objections from the Kerala High Court Advocates' Association, citing concerns over access to justice and procedural overreach.

Maharashtra launches MahaCrimesOS AI to strengthen cybercrime investigation and digital safety

Microsoft, in collaboration with the Government of Maharashtra, its special purpose vehicle, MARVEL, and cybersecurity firm CyberEye, unveiled MahaCrimeOS AI at the Microsoft AI Tour in Mumbai. Announced by Microsoft Chairman and CEO Satya Nadella, the Azure-powered platform is designed to support cybercrime investigations

[3] Blue Star Aluminium & Door House v. Federal Bank & Anr., WP(C) No. 43123/2025.

through AI-assisted workflows, multilingual data extraction, contextual legal assistance, and secure cloud infrastructure.

Currently live in 23 police stations in Nagpur, the system has been proposed for expansion to all 1,100 police stations across Maharashtra, as endorsed by Chief Minister Devendra Fadnavis. Built on Microsoft Azure OpenAI Service with embedded compliance and security safeguards, MahaCrimeOS AI reflects India's growing focus on deploying responsible AI in law enforcement while balancing investigative efficiency with data protection and privacy considerations amid rising cybercrime incidents nationwide.

JANUARY

Madras High Court blocks school students' personal data collection directive[4]

The Madurai Bench of the Madras High Court has struck down a Tamil Nadu government directive requiring government-run model schools to collect extensive personal and socio-economic data of higher secondary students. It held that the exercise violates the fundamental right to privacy. The Division Bench noted that the State failed to demonstrate any statutory basis or legitimate purpose for gathering sensitive information such as caste, gender identity, experiences of abuse, migratory status, and family circumstances. The Court observed that indiscriminate profiling of minors risks long-term discrimination and stigmatization.

The Court held that compelling students to disclose such information without safeguards or a clear necessity cannot be justified under Article 21. It emphasised that any State-led data collection involving children must be proportionate, backed by law, and accompanied by adequate privacy protections. Finding the exercise excessive and constitutionally infirm, the Bench quashed the September 2025 directive issued by the Education Department and directed the State not to undertake similar data-collection initiatives without legislative authorisation and privacy-preserving safeguards.

Kerala High Court closes pleas against Sprinklr data-sharing deal[5]

[4] Ameer Alam v. The Government of Tamil Nadu Ors., W.P.(MD) No. 29474/2025.
[5] Balu Gopalakrishnan v. State of Kerala & Ors. and connected matters, WP(C) No. 9498/2020 and connected cases.

The Kerala High Court has refused to entertain petitions challenging the State's engagement with a U.S.-based data analytics firm, Sprinklr Inc., for COVID-19 data management. The Court observed that there was "no ulterior motive" in entering into the contract and that the petitioner had failed to establish any legal or constitutional infirmity in the arrangement. The Division Bench emphasized that the contract was executed in the interest of public health during the pandemic and that the State had not acted arbitrarily or in breach of privacy norms.

The Court noted that patients' data was maintained on secured servers with access controls and that there was no evidence of misuse or commercial exploitation. The Court observed that Sprinklr's role was limited to assisting the Department of Health with data integration and analytics and found that the contractual terms did not involve unfettered access to personal data that could jeopardise privacy rights. After examining the pleadings, the Bench declined to grant any relief and closed the petitions, underlining that policy decisions made in the midst of a public health crisis would not be lightly interfered with in the absence of clear violations of law.

Supreme Court flags AI-generated fake evidence, false allegations in matrimonial disputes[6]

The Supreme Court of India has recognised the increasing use of fake and AI-generated evidence and false allegations in matrimonial disputes. It underscored the potential for such practices to distort justice rather than resolve marital conflicts. While dissolving a long-running marriage, the Bench observed that parties increasingly deploy technological means, including fabricated materials produced with AI, to strengthen spurious claims and gain leverage in litigation. The Court noted that when disputes escalate into extensive legal battles with hundreds of cases filed across forums, the objective often shifts from reconciliation to inflicting harm on the other side, with fabricated evidence becoming a common tool in that strategy.

The Bench emphasised that courts must prioritise mediation and reconciliation before allowing the exchange of allegations that aggravate hostility. It cautioned against the

[6] Neha Lal v. Abhishek Kumar, 2026 INSC 73.

routine invocation of criminal law for matters that could be resolved outside court. It acknowledged that the misuse of technology to create artificial evidence and false narratives not only damages the institution of marriage but also destroys lives, reputations, and careers when police involvement becomes a point of no return.

The judgment underlined that while judicial powers under Article 142 may dissolve irretrievably broken marriages, abuse of the legal system, whether through unverified evidence or coercive litigation, cannot be ignored, and mechanisms must be strengthened to deter such practices.

Madras High Court permits limited use of AI in arbitration proceedings[7]

The Madras High Court has authorised the restricted use of an AI-enabled platform, Superlaw Courts, in a set of arbitration matters involving the Gammon–OJSC Mosmetrostroy Joint Venture and Chennai Metro Rail Limited. The Court granted approval after the system was demonstrated in open court. The Court clarified that the tool may be used only to manage the extensive case records by helping retrieve, organise, and summarise existing documents. It stressed that the platform is not permitted to interpret facts, form opinions, or engage in any evaluative legal reasoning.

The Bench reiterated that judicial decision-making must remain entirely human-led. It directed that the proceedings be briefly paused so that both sides can acquaint themselves with the tool's functioning and verify any summaries or outputs generated. The Court also required that all AI-assisted material be independently checked by counsel before being placed on record. Through this measured approach, the Bench signalled that technological tools may assist the judicial process, but only under strict safeguards that preserve transparency, party confidence, and the primacy of human adjudication.

To view the full article please click here.

[7] Gammon-OJSC Mosmetrostroy JV v. Chennai Metro Rail Ltd., Arb O.P(COM. DIV.) No. 247/2022.