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

THE EVOLUTION OF CYBER LAW IN INDIA

~ Yutika Rachh

India's cyber law framework is built on a layered architecture of legislations, rules and regulatory directions that have evolved with the country's significant digital growth. At its foundation sits the Information Technology Act, 2000 India's primary cyber law legislation dealing with financial data safety, cybercrimes, e-commerce and more. The core objectives of the Act are: To enhance e-governance and improving digital government services, establishing cyber-security measures by imposing penalties on cyber-crime, regulating other cyber activities and finally, encouraging growth in India's IT and IT-enabled Services (ITES) sectors.

Some particularly transformative provisions of the Act include legal recognition of electronic records and digital signatures. Section 4 and 5 of the Act make it so that electronic records may be recognized in the same manner as paper-based documents and digital signatures as handwritten ones. This improves ease in online filing of documents, electronic issuance of licenses and approvals, digital payments and online contracts. The Act covers offences related to computers, computer systems and networks criminalizing hacking, data mining and theft, spreading computers viruses and malware, pornography and cyber terrorism. It gives the definition for an "Intermediary" which broadly includes telecom, network and internet service providers, webhosting providers, search engines, online payment and auction sites etc.[1] The Act extends to the whole of India, and to offences or contraventions committed outside India but where the relevant computer or network system in located in India.

This Act came as the legal green-light for India's digital economy, giving people and business the confidence and regulation needed to transact online.

---

[1] *Information Technology Act, 2000 (IT Act)*, GeeksforGeeks (last updated Mar. 26, 2026), https://www.geeksforgeeks.org/cybersecurity/information-technology-act-2000-india/.

Over a decade later, the Indian Computer Emergency Response Team (CERT-In) introduced its cyber security directions. CERT-In is an office within the Ministry of Electronics and Information Technology. It is the nodal agency to deal with cyber security incidents and mount a defense in the Indian Internet domain. India witnessed an alarming number of cyber security issues and data breach incidents from 2020-22 which prompted the release of the CERT-In Cyber Security Directions of 2022 which strengthened India's incident-response procedures.

Every covered entity must report breaches or security violations to CERT-In within 6 hours of their of becoming aware of them and this overrides any contractual confidentiality entities may have with their customers. Entities must also maintain 180-day rolling logs of ICT-systems within India while logs may sometimes be stored outside India, the entity must be able to produce them before CERT-In within a reasonable amount of time.[2] All ICT system clocks also have to be synchronized to the Network Time Protocol (NTP) servers of the National Informatics Centre (NIC) or the National Physical Laboratory (NPL), or to NTP servers traceable to these sources, ensuring standardized timestamps critical for forensic investigation and cross-entity incident correlation. VPS, VPN, cloud storage providers and all entities in the virtual asset ecosystem were now subjected to stricter KYC and data localisation obligations including storage of names, IP addresses and usage patterns for 5 years. All service providers, even those without a physical presence in India, had to appoint a Point of Contact to liaise with the CERT-In office.[3]

Alongside this came the Digital Personal Data Protection Act, 2023. It traces back to the landmark Supreme Court ruling in Justice K.S. Puttasawamy (Retd.) and Anr. v. Union of India, 2017, where it was held that the Right to Privacy is included in Article 21 and Part III of the Indian Constitution. Following this a committee of experts, chaired by Justice B.N. Srikrishna was formed in 2018 to recommend a comprehensive digital data protection framework for India resulting in the DPDP Act of 2023.

---

[2] Neeti Biyani, Andrei Robachevsky & Prateek Waghre, *Internet Impact Brief: India CERT-In Cybersecurity Directions 2022*, Internet Soc'y (June 1, 2022), https://www.internetsociety.org/resources/doc/2022/internet-impact-brief-india-cert-in-cybersecurity-directions-2022/

[3] *The CERT-In Cyber Security Directions: More Questions Than Answers*, Cyril Amarchand Mangaldas Blog (May 2022), https://corporate.cyrilamarchandblogs.com/2022/05/the-cert-in-cyber-security-directions-more-questions-than-answers/.

The Act defines digital personal data as data in a digital form in relation to a person or by which that person may be identified. It establishes two key roles: Data Principals – individuals whose personal data is being processed and Data Fiduciaries – entities that determine the purpose and means of processing.[4] All fiduciaries are required to obtain informed consent before collecting personal data, ensure data accuracy, maintain reasonably safeguards and report any breaches to the Data Protection Board of India. This Board adjudicates disputes between principals and fiduciaries. Conversely, principals are given the right to obtain information about how their data is being processed, to seek correction or deletion of data and grievance redressal. Significant Data Fiduciaries are designated based on the volume and sensitivity of the data they process.

The Act has a phased implementation with its second and third phases coming into force on 13th November 2026 and 13th July 2027 respectively.[5] It adopts a "Simple, Accessible, Rational and Actionable" (SARAL) approach making law easy to understand and implement.

The most recent and far-reaching development in this landscape is the Information Technology (Intermediary Guidelines and Digital Media Ethics Code), Rules 2021 and their 2026 Amendment. The 2021 rules supersede India's Intermediary Guidelines Rules of 2011. They significantly widened the scope of intermediary oversight by bringing online news content and Over-The-Top (OTT) Platforms under its purview. The rules stem from Section 87 of the IT Act, 2000 and introduce two new classes of intermediaries: Social media intermediaries and Significant social media intermediaries (SSMIs). The government may define different thresholds under these categories and entities may be subject to varying levels of obligation.[6]

All intermediaries are required to publish their rules, regulations, privacy policy and user agreements, prominently on their website or app and prohibited content categories must be notified to users. SSMIs must comply to a three-tier due diligence system i.e. a Chief

---

[4] Lalit Kalra, *Decoding the Digital Personal Data Protection Act, 2023*, EY (Nov. 21, 2025), https://www.ey.com/en_in/insights/cybersecurity/decoding-the-digital-personal-data-protection-act-2023.

[5] Charmian Aw & Ciara O'Leary, *India's Digital Personal Data Protection Act 2023 Brought into Force*, Hogan Lovells Cadwalader (Nov. 17, 2025), https://www.hlc.com/en/publications/indias-digital-personal-data-protection-act-2023-brought-into-force-.

[6] PRS Legislative Research, *The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021*, PRS India (Feb. 25, 2021), https://prsindia.org/billtrack/the-information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-2021.

Compliance Officer, a Nodal Contact Person and a Resident Grievance Officer and publish monthly compliance reports. OTT platforms must follow self-classification model based on content ratings and further sub-classify content with sensitive themes such as, violence, nudity, substance abuse.[7]

While these 2021 rules prohibit impersonation, obscenity, misinformation and privacy violations they don't consider hyper-realistic video and voice cloning or large-scale synthetic text which has now become a part of mainstream media. As deepfake tools became widely available and incidents of AI-powered financial fraud, non-consensual intimate imagery, political misinformation, and executive impersonation increased, enforcement under the present framework became interpretive rather than explicit.

The 2026 Amendment Rules address this gap by formally introducing the concept of "Synthetically Generated Information" and a two-tier compliance structure depending on whether an intermediary merely hosts SGI or assists in its creation, storage, transmission and dissemination.[8] The amendment creates a transparency obligation to ensure that AI-generated content does not fall under a prohibited category and is disclosed correctly, aiming to reduce the risk of deception. The new rules require rapid action: three hours for AI-generated content to be deemed illegal by a Court subsequently taken-down, two hours in case of sensitive violations such as non-consensual deepfake nudity.

The amendment creates accountability and India-specific compliance obligations for global platforms inclusive of social media and OTT. The SGI framework is India's first comprehensive statutory regulation of deepfakes and other synthetic media and sets a precedent that other jurisdictions are actively studying.[9]

---

[7] TNM (with ANI Inputs), *India Enforces New Rules on Deepfakes and AI-Generated Content from February 20*, The News Mill (Feb. 20, 2026), https://thenewsmill.com/2026/02/india-enforces-new-rules-on-deepfakes-and-ai-generated-content-from-february-20/

[8] Prashant Mali, *AI Laws and Regulations in India as of 2026: A Comprehensive Overview for Practitioners, Businesses, and Policymakers*, Cyber L. Blog India (Feb. 2026), https://www.prashantmali.com/cyber-law-blog-india/ai-laws-and-regulations-in-india-as-of-2026.

[9] Vedant Choudhary & Ankit Chugh, *India's 2026 Amendment to IT Rules: Regulation of Deepfakes, AI Content and the Three-Hour Takedown Regime*, SKV L. Offices (Feb. 19, 2026), https://skvlawoffices.com/indias-2026-amendment-to-it-rules-regulation-of-deepfakes-ai-content-and-the-three-hour-takedown-regime/

All in all, cyber law in India appears to have a wide and comprehensive scope but as the technological landscape changes and evolves, some gaps and missing links are bound to appear.[10] It is necessary to identify structural reforms that can further align it to global standards and live up people's digital needs.

The lack of unification is a major fallacy that presents itself here. The same sets of users and institutions, principals and intermediaries are subjected to multiple regulations that often serve an identical purpose. If consolidated into one coherent statute, this patchwork of legislations becomes easier to understand, execute and comply with. It also becomes more adaptable and there is ease of introducing future amendment. It is understandable that sector-specific regulations are required but maintaining a national cybersecurity baseline standard to which all of them must conform at minimum, reduces the compliance complexity and still permits sectoral regulators to impose higher standards where the risk profile demands it.

The approach taken by the European Union's NIS2 Directive can be mirrored; it identifies 18 critical sectors and calls on member states to develop their own cyber security strategies while specifying which policies it should include for instance: Supply chain security, vulnerability management, cybersecurity education and awareness.[11] On supply chain security, Indian laws currently address obligations of individual entities but lack insight on the security standards of vendors and third-party providers which some entities rely upon heavily. This is a greatly exploited vulnerability, purchasers and infrastructure operators must mandatorily conduct supply chain risk assessment to avoid the search for curative solutions in the future. Cybersecurity awareness and talent retention should also be introduced as an initiative. There should be a training requirement in this domain for public sector and regulated private sector enterprises. Through this, breaches and threats can be mitigated, identified and resolved much faster.

[10] *A Comparison of Cybersecurity Regulations: India*, PwC (Feb. 16, 2023), https://www.pwc.com/id/en/pwc-publications/services-publications/legal-publications/a-comparison-of-cybersecurity-regulations/india.html

[11] *NIS2 Directive: Securing Network and Information Systems*, Eur. Comm'n: Shaping Eur.'s Digital Future (last updated Jan. 20, 2026), https://digital-strategy.ec.europa.eu/en/policies/nis2-directive.

REFERENCES

1. Prashant Mali, *AI Laws and Regulations in India as of 2026: A Comprehensive Overview for Practitioners, Businesses, and Policymakers*, Cyber L. Blog India (Feb. 2026), https://www.prashantmali.com/cyber-law-blog-india/ai-laws-and-regulations-in-india-as-of-2026.

2. Charmian Aw & Ciara O'Leary, *India's Digital Personal Data Protection Act 2023 Brought into Force*, Hogan Lovells Cadwalader (Nov. 17, 2025), https://www.hlc.com/en/publications/indias-digital-personal-data-protection-act-2023-brought-into-force-.

3. Lalit Kalra, *Decoding the Digital Personal Data Protection Act, 2023*, EY (Nov. 21, 2025), https://www.ey.com/en_in/insights/cybersecurity/decoding-the-digital-personal-data-protection-act-2023.

4. PRS Legislative Research, *The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021*, PRS India (Feb. 25, 2021), https://prsindia.org/billtrack/the-information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-2021.

5. TNM (with ANI Inputs), *India Enforces New Rules on Deepfakes and AI-Generated Content from February 20*, The News Mill (Feb. 20, 2026), https://thenewsmill.com/2026/02/india-enforces-new-rules-on-deepfakes-and-ai-generated-content-from-february-20/.

6. Vedant Choudhary & Ankit Chugh, *India's 2026 Amendment to IT Rules: Regulation of Deepfakes, AI Content and the Three-Hour Takedown Regime*, SKV L. Offices (Feb. 19, 2026), https://skvlawoffices.com/indias-2026-amendment-to-it-rules-regulation-of-deepfakes-ai-content-and-the-three-hour-takedown-regime/.

7. Neeti Biyani, Andrei Robachevsky & Prateek Waghre, *Internet Impact Brief: India CERT-In Cybersecurity Directions 2022*, Internet Soc'y (June 1,

2022), https://www.internetsociety.org/resources/doc/2022/internet-impact-brief-india-cert-in-cybersecurity-directions-2022/.

8. *The CERT-In Cyber Security Directions: More Questions Than Answers*, Cyril Amarchand Mangaldas Blog (May 2022), https://corporate.cyrilamarchandblogs.com/2022/05/the-cert-in-cyber-security-directions-more-questions-than-answers/.

9. *A Comparison of Cybersecurity Regulations: India*, PwC (Feb. 16, 2023), https://www.pwc.com/id/en/pwc-publications/services-publications/legal-publications/a-comparison-of-cybersecurity-regulations/india.html.

10. Tejas Bharadwaj, *Mapping India's Cybersecurity Administration in 2025*, Carnegie Endowment for Int'l Peace (Sept. 1, 2025), https://carnegieendowment.org/research/2025/09/mapping-indias-cybersecurity-administration-in-2025.

11. *Information Technology Act, 2000 (IT Act)*, GeeksforGeeks (last updated Mar. 26, 2026), https://www.geeksforgeeks.org/cybersecurity/information-technology-act-2000-india/.

12. Prince Kumar, *The Evolution of India's Information Technology Act 2000: A Comprehensive Guide*, Journalism Univ. (Jan. 9, 2026), https://journalism.university/media-ethics-and-laws/evolution-india-information-technology-act-2000-guide/.

13. *NIS2 Directive: Securing Network and Information Systems*, Eur. Comm'n: Shaping Eur.'s Digital Future (last updated Jan. 20, 2026), https://digital-strategy.ec.europa.eu/en/policies/nis2-directive.

14. The Information Technology Act, No. 21 of 2000, India Code (2000).

15. The Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).