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

CYBERSECURITY LAWS IN INDIA

~ Alena Mary Jacob

The Information Technology (IT) Act, 2000, is the primary legislation dealing with cybersecurity, data protection and cybercrime. Its key features include, granting statutory recognition and protection to electronic transactions and communications, and identifying activities such as hacking, denial-of-service attacks, phishing, and malware attacks as punishable offences.[1] As per the National Cyber Crime Reporting Portal of the Government of India, cybercrime may be defined as *"Any unlawful act where computer or communication device or computer network is used to commit or facilitate the commission of crime".*[2]

Cybersecurity is rapidly emerging as one of the critical areas in the global digital ecosystem, especially as companies expand their dependence on cloud platforms and artificial intelligence (AI). The rising significance also signals the need for skilled professionals, where India may be lacking. According to a new report by the Data Security Council of India (DSCI) and the SANS Institute, India is facing a sharp shortage of skilled cybersecurity professionals, with 73 per cent of enterprises and 68 per cent of service providers reporting limited availability of qualified talent. The latest '*Indian Cyber Security Skilling Landscape Report 2025–26*' underscores a widening gap between the rapid pace of digital transformation and workforce readiness. The report found that 84 per cent of companies take around one to six months to fill cybersecurity roles. This points at the persistent hiring challenges across the sector. As per the report, around 63 per cent of enterprises and 59 per cent of providers claimed that job applicants lack hands-on practical skills. Additionally, nearly 58 per cent of enterprises and 60 per cent of providers admitted that they struggle to find professionals with cross-domain expertise in cloud, applications, and identity systems. The report attributes these gaps to a structural shift

[1] PricewaterhouseCoopers, *A Comparison of Cybersecurity Regulations: India* (2025). https://www.pwc.com/id/en/pwc-publications/services-publications/legal-publications/a-comparison-of-cybersecurity-regulations/india.html (last visited May 19, 2026).

[2] Government of India, *National Cyber Crime Reporting Portal*. https://www.cybercrime.gov.in/Accept.aspx (last visited May 15, 2026).

in enterprise technology environments, as organizations focus on cloud-native platforms, API-driven architectures, and AI-enabled operations.[3] *Lt. Gen. Madhavan Unnikrishnan Nair*, Chairman, 63SATS said, *"As digital adoption becomes universal, cyber threats are increasingly using AI to exploit vulnerabilities, especially at the interface of human behavior and connected devices."* At the same time, he added that artificial intelligence was proving to be a powerful enabler for cybersecurity by improving efficiency and strengthening threat detection. *"The focus going forward should be on using AI responsibly to simplify processes, enhance security, and build a more resilient digital ecosystem,"* he emphasized. *"In a country like India, with over 1.4 billion Aadhaar identities driving digital transactions, secure and consent-based authentication becomes critical. The shift towards mechanisms such as face authentication and controlled data sharing is an important step in reducing fraud and giving users greater control over their identity,"* he said while speaking at CyberSec India Expo (CSIE) 2026 organized by Media Fusion in Mumbai.[4] With the speedy evolution of India's digital ecosystem, legal accountability has also expanded from individual offenders to false digital mediators. In the case of ***Avnish Bajaj v. State (NCT of Delhi) (2008),*** which highlighted the legal uncertainty regarding the responsibility of online platforms, especially the safe-harbor protection provided to intermediaries under *Section 79*. The Delhi High Court examined, whether an intermediary could be held criminally liable for user-generated content. The case became a landmark in defining intermediary liability under Section 79 of the Information Technology Act, establishing that while digital platforms may receive statutory protection, they must exercise due diligence and cannot entirely avoid responsibility for unlawful activities conducted through their services.[5] With the growing volume of personal and enterprise data, achieving the right balance between privacy and security remains critical, supported by frameworks such as the DPDP Act. There is a growing need to establish clear 'rules of the digital highways', including stronger identity frameworks for devices and users to ensure trusted access. As cyber risks evolve, safeguarding digital infrastructure must be viewed as a shared responsibility, where every citizen plays a role in securing the nation's cyber

[3] Indian Express, *India's Cybersecurity Skills Gap Widens as AI Demand Surges* (2025). https://indianexpress.com/article/technology/artificial-intelligence/india-cybersecurity-skills-gap-ai-demand-report-10665764/ (last visited May 15, 2026).

[4] "India's Cybersecurity Market Set to Grow to $150.6 Billion by 2031 as Companies Invest to Fend Off Sophisticated Cyber Attacks," Lalatendu Mishra, The Hindu (2026) https://www.thehindu.com/business/indias-cybersecurity-market-set-grow-to-1506-billion-by-2031-as-company-invest-to-fend-off-sophisticated-cyber-attacks/article70902974.ece/amp/ (last visited May 15, 2026).

[5] Avnish Bajaj v. State (NCT of Delhi), 116 (2005) DLT 427.

ecosystem. Recently, several X and Meta users have reported that their posts and accounts were blocked in India following government orders issued under *Section 69A of the Information Technology Act, 2000*. According to reports, affected users received automated notifications, stating that their posts had been blocked in response to a legal demand attributed to the Ministry of Electronics and Information Technology, but no explanation was provided for the action. These blocking orders highlight a broader problem with India's internet blocking regime. *Section 69A of the Information Technology Act*, permits the government to block online information only on specific grounds, such as sovereignty, national security, public order, or the prevention of incitement to offences.[6] In the landmark case of ***Shreya Singhal v. Union of India (2015),*** where Shreya Singhal, a law student had challenged *Section 69A of the IT Act*, considering the punishment for sending online messages as *"grossly offensive," "menacing,"* or causing *"annoyance" or "inconvenience."* The wording was very broad and police used it in several controversial arrests. The Supreme Court in its judgement, held that *Section 66A* violated *Article 19(1)(a*) of the Indian Constitution (freedom of speech and expression). The Court said terms like *"annoyance"* and *"inconvenience"* were vague and could be misused to suppress legitimate online expression.[7] The Delhi High Court in ***Tanul Thakur v. Union of India (2023)***, emphasized the need for transparency regarding blocking orders. In this case, a satirical website was blocked under Section 69A without providing a hearing notice or a copy of the blocking order. The court directed the government to provide the petitioner with the blocking order and ordered that a post-decisional hearing be granted. While the Supreme Court has set out procedural safeguards, the Karnataka High Court's shift away from the narrow, safeguards-oriented reading of Section 69A adopted in Shreya Singhal has enabled the government to carry out this level of blocking. The **Cyber Crime Prevention against Women and Children (CCPWC)** is an important initiative taken by the government to address various forms of cybercrimes against women and children. However, about 76% of women under age 30, of the 500 million internet users in India, were victims of online harassment and 1 in 10 under the same age group had been the targets of "revenge porn and/or sextortion". In 2017, the CCPWC documented 135 deaths due to the Blue Whale suicide challenge game and three deaths due to the Momo challenge game. The Indian government took note of the urgency of the situation and contacted Google, Facebook, WhatsApp, Microsoft, and Yahoo and asked

[6] Anmol Jain, *Blocked Without Explanation*, Verfassungsblog (2025), https://verfassungsblog.de/blocked-without-explanation/ (last visited May 15, 2026).

[7] Shreya Singhal v. Union of India, (2015) 5 SCC 1.

them to immediately remove any links to such games. The CCPWC also conducts research related to cybercrimes against women and children to protect them against cyberpornography, cyberbullying, online harassment, cyberstalking, matrimonial fraud, and banking fraud. Forensic laboratories operate at national and state levels. Training is provided to law enforcement, judges, and prosecutors on cybercrimes, with a special focus on women and children. The Ministry has also developed a handbook on cybersecurity for young people and the government has disseminated computer policy and guidelines to all concerned departments. Globally, access to the Internet has grown exponentially, and India is no exception. With the increase in access to technology, including cell phones, computers, and other electronic devices, countries around the world are grappling with the problem of regulating abuse of technology and related criminal activities. Until recently, India had relied on outdated laws such as the Information Technology Act (IT Act) 2000, the Bharatiya Nyaya Sanhita and formerly the Indian Penal Code (IPC), and the Indian Copy Right Act of 1957 to address copyright infringement, trademark infringement, to a wide range of cybercrimes including identify theft, credit card fraud, computer hacking, cyberbullying, extortion, distribution child pornography, and cyber-terrorism. One of the earliest and most significant cases, that shaped the legal response to online speech, cybercrime and intermediary liability was ***State of Tamil Nadu v. Suhas Katti,*** which became the first successful conviction under the Information Technology Act, 2000. The conviction in this case demonstrated that cyber offences such as online harassment and misuse of digital communication could be effectively prosecuted under Indian law. Thereby, establishing that offences committed in cyberspace could be effectively prosecuted through existing legal mechanisms.[8]

As of 17th of May, 2026 in its continuing enforcement of cyber laws, the Mizoram Police had arrested two individuals for allegedly uploading obscene and sexually explicit content through YouTube channels. Authorities invoked Section 67 of the Information Technology Act, 2000 along with Section 294 of the Bharatiya Nyaya Sanhita, indicating that Indian cyber regulation continues to rely on a combination of digital legislation and general criminal law to address online offences.[9] India is preparing to overhaul its cybersecurity architecture as the government weighs a new legal framework to tackle the rapidly evolving threat landscape shaped by

[8] Sakshi Vadhera & Nikita Sharma, Case Commentary: State of Tamil Nadu v. Suhas Katti, SSRN (2021).
[9] India Today NE, *Two Arrested in Mizoram for Allegedly Uploading Obscene Content on Social Media*. https://www.indiatodayne.in/mizoram/story/two-arrested-in-mizoram-for-allegedly-uploading-obscene-content-on-social-media-1393074-2026-05-17 (last visited May 17, 2026).

artificial intelligence. Speaking at the launch of the AI & Cyber Threat Research Center during the India AI summit in New Delhi, *Union IT Minister Ashwini Vaishnaw* underscored the urgency of moving beyond traditional cyber defence models.[10]

[10] Moneycontrol, *India Weighs Fresh Cyber Law Amid Rising AI-Led Threats; Airtel, Zscaler Set Up Research Center* (2025). https://www.moneycontrol.com/news/business/information-technology/india-weighs-fresh-cyber-law-amid-rising-ai-led-threat-airtel-zscaler-set-up-research-center-13837989.html (last visited May 15, 2026).