THE REDWOOD JOURNAL

Website: www.the redwood journal.com

VOLUME:-5 ISSUE NO:-5 , SEPTEMBER 7, 2026

ISSN (ONLINE):- 3139-7360

Email: theredwoodjournal@gmail.com

Digital Number : 2025-23534643

CC BY-NC-SA

Authored By:- Shambhavi Singh

Amity Law School, Amity University Patna, Bihar

EMERGING CYBERSECURITY THREATS AND LEGAL CHALLENGES IN INDIA

Abstract

India now lives much of its life online. We pay through UPI, bank on our phones, file government forms from home and see doctors over video calls. That shift has opened real opportunities, but it has also handed criminals, hostile states and opportunists a much larger target. Ransomware, phishing, identity theft, financial fraud, AI-enabled scams and deepfakes are no longer rare events. They affect national security, the economy and ordinary people's privacy. The country's legal response rests mainly on the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, institutions such as CERT-In, and a patchwork of directions and policies. That foundation matters, but newer technologies have exposed gaps in accountability, coordination between agencies, protection of critical infrastructure, privacy and day-to-day enforcement. This article traces how India's cybersecurity framework developed, looks at the threats that now shape it, examines data protection, compares India with the EU, Singapore and Japan, and ends with practical reforms for a framework that is comprehensive, adaptable and respectful of rights.

Keywords: *Cybersecurity, Cyber Law, Information Technology Act 2000, Artificial Intelligence, Deepfakes, Data Protection, Digital Privacy, Cybercrime, Digital Forensics, Critical Infrastructure*

Introduction

Digital technology has changed how India works. Digital payments, online banking, e-commerce, e-governance, health technology and everyday communication have boosted the economy, made public services easier to reach and put information within almost everyone's grasp. But the more we depend on digital infrastructure, the more exposed we become. Individuals, businesses and government bodies all face growing cyber threats.

Cybersecurity means protecting computer systems, networks, devices and information from unauthorised access, misuse, damage, disruption or destruction. It is no longer only a technical matter. It touches national security, economic development, privacy, public safety and constitutional rights.

India's main law in this field is the Information Technology Act, 2000. It was written mainly to give legal recognition to electronic records and transactions and to deal with certain offences involving computers and networks. Since then, artificial intelligence (AI), the Internet of Things (IoT), cloud computing, blockchain, cryptocurrency, 5G and quantum computing have introduced risks the original drafters could not fully have foreseen.

Over the years India has built a set of institutions to respond: the Indian Computer Emergency Response Team (CERT-In), the National Cyber Security Coordinator (NCSC), the National Critical Information Infrastructure Protection Centre (NCIIPC), the Defence Cyber Agency and the National Cyber Security Policy, 2013. The Digital Personal Data Protection Act, 2023, followed by the Digital Personal Data Protection Rules, 2025, is the latest major addition.

Still, laws alone do not make a country secure. Results depend on how well institutions coordinate, how prepared the technology is, whether enforcement agencies have the capacity to act, and how aware the public is. India's challenge is to protect digital systems and personal information without choking innovation or trampling constitutional freedoms.

1.1 The problem

Despite the progress, cyber threats keep growing in sophistication. Existing provisions may not fully answer problems raised by AI-generated deepfakes, automated attacks, ransomware, cross-border crime and attacks on critical infrastructure. Scattered institutional responsibilities, a shortage of technical expertise, difficulty in collecting digital evidence and privacy concerns make enforcement harder still.

The central question is this: is India's current cybersecurity framework equipped to handle emerging threats while keeping a fair balance between national security, individual privacy and technological growth?

1.2 What this article sets out to do

- Trace how cybersecurity law and policy have evolved in India.
- Identify emerging threats, especially AI-enabled crime and financial fraud.
- Assess how far the DPDP Act, 2023 protects digital privacy.

- Pinpoint legal, institutional and enforcement gaps.
- Examine the challenges posed by new technologies.
- Show why digital forensics and skilled professional's matter.
- Suggest legal and policy reforms.

1.3 Questions explored

- Is the IT Act, 2000 enough to deal with emerging threats?
- What legal problems arise from AI-enabled crime and deepfakes?
- How well does the DPDP Act, 2023 protect privacy and personal data?
- What are India's main institutional and enforcement challenges?
- Which reforms would build a truly comprehensive framework?

1.4 Method

The study is doctrinal and analytical. It draws on secondary sources: statutes, government policies, official notifications, court decisions, research articles, books, reports and international legal frameworks. It looks closely at the IT Act, 2000 and the DPDP Act, 2023, studies India's institutions, and compares selected features with the EU's GDPR, Singapore's PDPA and Japan's cybersecurity framework. The approach is qualitative, aimed at spotting legal gaps and proposing workable reforms.

2. How India's Cyber Framework Evolved

India's cyber regulation has grown hand in hand with information technology and online commerce. The IT Act, 2000 laid the foundation by recognising electronic records and electronic signatures and by creating offences such as unauthorised access and damage to computer systems.

The Information Technology (Amendment) Act, 2008 strengthened the law. It added or revised provisions on identity theft, cheating by personation, violation of privacy, cyber terrorism and intermediary liability. After that, the country developed specialised institutions and policies for incident reporting, cyber defence and critical infrastructure protection.

Milestone	What it did
IT Act, 2000	Foundation of India's cyber-law framework
IT Amendment Act, 2008	Added offences and broadened the framework
National Cyber Security Policy, 2013	Set a wider vision for securing cyberspace
CERT-In	National agency for responding to cyber incidents
NCIIPC	Protects critical information infrastructure

Milestone	What it did
DPDP Act, 2023	Statutory framework for processing digital personal data
DPDP Rules, 2025	Detailed rules to implement the data-protection framework

In short, India has moved from regulating electronic transactions and cyber offences towards a broader system that covers digital security, privacy and national cyber preparedness.

3. The Threats We Face Today

Technology is moving fast, and so are the people who abuse it. The threats below can hit individuals, companies, government bodies and national infrastructure alike.

3.1 Ransomware and advanced persistent threats

Ransomware is malicious software that locks users out of their systems or data, usually by encrypting it, and demands payment to restore access. Some attackers also steal confidential data and threaten to leak it unless they are paid. Picture a hospital hit by ransomware: doctors lose access to patient records, diagnostics and appointment systems, essential care is interrupted and lives may be put at risk.

An advanced persistent threat (APT) is a sophisticated attack in which the intruder gets into a network and quietly stays there for a long time. Typical targets include government departments, defence establishments, financial institutions, research bodies and critical infrastructure. State-sponsored attacks are especially worrying because they may be tied to espionage, intelligence gathering or strategic disruption.

> *Legal angle: Such incidents can involve unauthorised access, data theft and damage to computer systems under Sections 43 and 66 of the IT Act. Where the requirements are met, other provisions, including Section 66F on cyber terrorism, may also apply.*

3.2 AI-enabled cybercrime and deepfakes

AI is a useful tool for society, but criminals use it too. AI-enabled cybercrime covers unlawful activity in which AI helps carry out fraud, identity theft, manipulation, cyberattacks or the creation of misleading content. The main forms are:

- **AI-generated phishing.** Convincing fake emails, messages and websites that steal passwords and banking details.
- **Social engineering.** Imitating the way trusted people write or speak, then pressuring victims through fear, urgency or emotion.
- **Deepfake video and voice.** Artificially generated or manipulated material that makes it seem someone said or did something they never did.
- **Identity theft.** AI-generated images, cloned voices and doctored identity documents used to impersonate people.

- **Financial fraud.** Posing as company directors, bank officials or family members to persuade victims to transfer money.
- **Automated malware.** AI helping attackers find vulnerabilities, tweak malicious code and automate attacks.
- **Disinformation.** False AI-generated content spread to sway opinion, damage reputations or stir social tension.

Deepfakes are particularly damaging because they erode trust in digital communication and can seriously harm dignity, privacy and reputation.

Legally, the IT Act already has provisions that can apply to deepfake-related conduct, depending on the facts. These include Sections 66C, 66D, 66E, 67 and 67A, and relevant provisions of the Bharatiya Nyaya Sanhita, 2023 may also apply. But India has no single statute that regulates all forms of AI-generated deepfakes. That leaves a need for clearer rules on accountability, consent, liability and remedies.

3.3 Financial fraud and social engineering

UPI, mobile banking and digital wallets have brought millions into the formal financial system. They have also created new openings for fraud. Common methods include:

- **Phishing:** fraudulent emails, messages or links that harvest banking and personal details.
- **Vishing:** fake phone calls from supposed banks, government departments or other trusted bodies.
- **SIM swapping:** taking over a victim's mobile number to intercept OTPs and authentication messages.
- **QR-code and UPI fraud:** fake QR codes, misused payment requests or misleading instructions that trigger unauthorised payments.
- **ATM skimming:** hidden devices that capture card data and sometimes PINs.
- **Identity theft:** using stolen personal data to get loans, open accounts or make transactions.
- **Investment and Ponzi scams:** promising unrealistic returns and paying early investors with money from new ones.

What makes social engineering so effective is that it targets human behaviour rather than technical weaknesses. Victims are pushed by fear, greed, urgency or misplaced trust. Depending on the facts, Sections 66C and 66D of the IT Act and the relevant provisions of the BNS may apply.

3.4 Critical infrastructure and nuclear security

Critical infrastructure means the physical and digital systems whose failure would seriously affect national security, public safety and the economy. Think of electricity grids, telecommunications, banking and financial systems, defence networks, transport, nuclear facilities and healthcare. An attack on a grid-management system, for instance, could cut power to hospitals, factories, transport and communications all at once.

Nuclear facilities need especially strong protection, because their digital systems may hold sensitive operational data and safety-related controls. Any compromise could create grave national-security and public-safety concerns.

India has set up the NCIIPC to protect critical information infrastructure. The IT Act supports this through Section 70, which deals with protected systems, and Section 70A, which provides for the national nodal agency. Cyber forensics also plays a vital role after an incident by tracing the source, preserving electronic evidence and reconstructing what happened.

4. Data Protection and Privacy

People hand over personal details to banks, schools, hospitals, government offices and online platforms every day. That data fuels economic and technological growth, but misusing it can lead to identity theft, fraud, surveillance and privacy violations. This is why data protection is now a core part of India's cybersecurity framework.

4.1 The Digital Personal Data Protection Act, 2023

The DPDP Act sets out a legal framework for processing digital personal data in India. It tries to balance two aims: protecting individuals' privacy and personal information, and letting organisations process data for lawful purposes. It introduces the ideas of Data Principals (the individuals) and Data Fiduciaries (those who decide why and how data is processed), and sets obligations around consent, security, processing and accountability.

Consent

Consent must be free, specific, informed, unconditional and unambiguous, and must involve a clear affirmative action. When you sign up on a shopping platform, for example, the platform must tell you how your data will be used and obtain consent where consent is the applicable basis. Consent can also be withdrawn.

Processing

Processing covers any operation on personal data, wholly or partly by automated means: collecting, recording, organising, storing, using, analysing, sharing, disclosing, updating and erasing. A bank that collects a customer's name, phone number and financial details, stores them and uses them to provide services is processing personal data.

What Data Fiduciaries must do

Banks, hospitals, schools and e-commerce firms are typical Data Fiduciaries. Their main duties include:

- Processing personal data in line with the Act.
- Giving Data Principals the required information.
- Maintaining appropriate security safeguards.
- Taking reasonable steps to prevent personal data breaches.
- Complying with erasure requirements.
- Setting up grievance-redressal mechanisms.

- Meeting extra obligations if classed as a Significant Data Fiduciary.

Rights of Data Principals

- **Access:** obtain information about their personal data and how it is processed.
- **Correction:** ask for inaccurate or misleading data to be corrected.
- **Erasure:** ask for data to be erased, subject to legal requirements.
- **Grievance redressal:** complain through the prescribed mechanism.
- **Nomination:** nominate someone to exercise their rights in case of death or incapacity.

Security and penalties

Data Fiduciaries must put reasonable security safeguards in place, such as encryption, strong passwords, access controls, security audits and backups. The Act provides monetary penalties for specified breaches. Failing to maintain reasonable security safeguards, for example, can attract a penalty of up to ₹250 crore. The Data Protection Board of India handles specified contraventions and imposes penalties under the Act.

> *An important caveat on timing: The DPDP Rules, 2025 were notified on 14 November 2025, but the Act and Rules come into force in phases. As of 2 November 2026, most substantive data-processing obligations and individual rights are scheduled to commence 18 months after notification, in May 2027, although some provisions start earlier. It would therefore be inaccurate to describe the whole framework as already operational.*

4.2 Practical hurdles in implementation

The DPDP Act is a strong legal foundation, but putting it into practice will be costly and complicated, especially for Micro, Small and Medium Enterprises (MSMEs).

- **IT infrastructure.** Secure servers, updated software, firewalls and encryption are expensive, and small businesses may struggle to afford them.
- **Employee training.** Staff need to understand confidentiality and data protection. Without that, weak passwords and accidental disclosures are likely.
- **Data management.** Organisations must know what personal data they hold, where it sits, why it is processed and how long it should be kept. Poor record-keeping raises breach risk.
- **Compliance systems.** Internal policies, grievance procedures, security monitoring and processes for handling data requests may need specialist legal and technical help.
- **Privacy and security procedures.** Clear steps for obtaining consent, protecting data, reporting breaches and blocking unauthorised access.

Large corporations usually have far more money and technical muscle than small firms, so compliance costs may fall unevenly across the economy.

4.3 How India compares: GDPR and Singapore's PDPA

Looking abroad helps show where India's framework is strong and where it falls short. The EU's General Data Protection Regulation (GDPR) is a comprehensive regulation that applies within the EU and, in some circumstances, to organisations outside it. It rests on principles such as lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability. It also recognises data portability and has a specific framework for automated individual decision-making.

Singapore's Personal Data Protection Act (PDPA) governs how organisations collect, use and disclose personal data. It includes consent requirements, purpose limitation, protection and retention obligations, access and correction rights, and data-breach notification.

The table below offers a broad, simplified comparison. It is a general guide, not a substitute for reading each instrument.

Feature	India (DPDP Act)	EU (GDPR)	Singapore (PDPA)
Core approach	Simplified framework for digital personal data	Detailed, rights-heavy regulation	Accountability and enforcement-driven model
Individual rights	Access, correction, erasure, grievance redressal, nomination	Wider set, including portability and rights on automated decisions	Access and correction rights
Regulator	Data Protection Board of India	Independent supervisory authorities in each member state	Personal Data Protection Commission
Breach notification	Required under the Act and Rules	Required, with set timelines	Required
Automated decisions	No dedicated framework	Specific safeguards	Not a central feature

The DPDP Act takes a more streamlined path than the GDPR, and differs in the breadth of individual rights, regulatory structure and safeguards for automated decision-making. The GDPR offers more detailed rights and supervisory machinery, while Singapore shows an alternative built on organisational accountability and active enforcement. India should learn from these models while keeping its own system consistent with its constitutional structure, economic needs and technological growth.

5. Gaps in the Legal Framework

India has built many laws, policies and institutions, yet fast-moving technology has exposed weak spots.

5.1 Definitional and regulatory gaps

The framework rests on several instruments: the IT Act, 2000, the DPDP Act, 2023, CERT-In Directions and sector-specific regulations. Emerging technologies raise questions these may not fully answer.

- **Artificial intelligence.** AI can be used to produce deepfakes, run automated fraud, manipulate information and aid cyberattacks. Existing laws may cover particular offences, but responsibility of developers, platform accountability and liability for harm need clearer rules.
- **Internet of Things.** Poorly secured connected devices can let attackers steal data or disrupt networks.
- **Cloud computing.** Storing data on remote servers raises questions of data ownership, jurisdiction, confidentiality, unauthorised access and who is responsible for a breach.
- **5G.** High-speed, interconnected networks support smart cities, connected vehicles and industrial automation, but also multiply the entry points for attack.
- **Critical infrastructure.** Grids, defence networks, nuclear facilities and telecom need specialised protection. A general cybercrime framework may not meet their security requirements.
- **Quantum computing.** It may one day break some of today's encryption. India must prepare with quantum-resistant cryptography and suitable security standards.

5.2 Institutional fragmentation

Cybersecurity depends on cooperation among government agencies, private organisations and technical institutions. India has several specialised bodies: CERT-In handles incident response, alerts and advisories; the NCSC offers strategic coordination; the NCIIPC focuses on critical information infrastructure; and the Defence Cyber Agency addresses defence needs. Each plays its part, but better coordination is needed across:

- Central and State governments, since incidents can cross state lines.
- Law-enforcement agencies, whose cybercrime units need technical support.
- Defence organisations, which must protect sensitive networks.
- Private companies, including banks, telecoms and technology platforms.
- Technology experts who find vulnerabilities and design defences.
- International organisations, because criminals often operate from abroad.

5.3 A lesson from Japan

Japan's Basic Act on Cybersecurity, 2014 treats cybersecurity as a shared responsibility of government, businesses and individuals. It stresses national coordination, protection of

critical infrastructure, information sharing, public-private cooperation, research and development, and international cooperation. Compared with a fragmented approach, an integrated system makes it easier to identify and manage risk. India can draw from this by strengthening coordination among its institutions, setting sector-specific security standards and improving information sharing between public and private bodies.

6. Emerging Technologies: Opportunity and Risk

New technology can strengthen security, but badly implemented, it can also add vulnerabilities.

6.1 Internet of Things

The IoT is a network of physical devices that connect to the internet to collect, exchange and process information: smartwatches, smart TVs, security cameras, home appliances, medical monitors, industrial sensors and smart-city systems. Many have limited processing power, outdated software or weak authentication. A smart camera protected by a weak password, for example, could let a hacker watch private activity.

Key security needs are confidentiality (only authorised people see the data), integrity (data is not altered without permission), authentication (devices and users prove who they are), protected data transmission and secure cloud infrastructure. IoT incidents can involve unauthorised access, privacy violations or data breaches under Indian law.

6.2 Blockchain

Blockchain is a distributed ledger in which information is recorded in linked blocks and maintained across a network. It can help security through decentralised record-keeping, data integrity (cryptography exposes unauthorised changes), permission-based access control, transparent audit trails and smart contracts, which are programmes that automatically carry out instructions when set conditions are met, such as releasing a payment once terms are verified.

But blockchain is not a cure-all. Smart-contract code can have flaws, private keys can be stolen, and privacy, scalability and regulatory uncertainty remain real concerns. It is best treated as a supporting technology, not a replacement for comprehensive cybersecurity.

6.3 Post-quantum cryptography

Today’s encryption systems, such as RSA and Elliptic Curve Cryptography, rely on mathematical problems that sufficiently powerful quantum computers could one day solve. Quantum computing is still developing, but the risk means we need to prepare now. Post-quantum cryptography aims to stay secure even against such machines. The main approaches are:

- **Lattice-based cryptography,** built on hard problems involving complex geometric structures called lattices; used for encryption and digital signatures.

- **Hash-based cryptography,** which builds secure digital signatures from the properties of hash functions.
- **Code-based cryptography,** which uses problems tied to error-correcting codes.

This matters for government communications, banking, defence information, healthcare records and any data that must stay confidential for years. India should encourage research and development and plan a gradual move to standardised quantum-resistant systems.

7. People and Enforcement

Laws and technology only work if trained people can use them. India faces a shortage of specialised cybersecurity professionals, particularly in law enforcement, digital forensics and advanced threat analysis.

7.1 The skills India needs

- **Cyber law experts** interpret cybercrime, data-protection and electronic-evidence law and advise on disputes.
- **Digital forensics experts** identify, collect, preserve and analyse electronic evidence.
- **Incident response specialists** investigate breaches and help organisations recover.
- **Malware analysts** study malicious software to learn how it works and how to remove it.
- **Ethical hackers** test systems with permission to find weaknesses before criminals do.
- **Data protection professionals** help organisations comply with privacy requirements.
- **AI security specialists** tackle risks such as data poisoning, model manipulation, AI-generated fraud and adversarial attacks.

7.2 Digital forensics, step by step

Digital forensics is the systematic process of identifying, collecting, preserving, examining and presenting digital evidence for investigations or legal proceedings. It is vital because so many crimes now happen through devices, networks and online platforms.

- **1. Identification.** Find potential sources of evidence: computers, phones, hard drives, CCTV, emails, server logs, cloud records and social media. In a banking fraud case, that might be the victim's phone, transaction records and related messages.
- **2. Preservation.** Protect the evidence from alteration or loss, document how it was handled and maintain a chain of custody recording who collected, transferred, stored and examined it.
- **3. Examination and analysis.** Experts use specialised tools to study deleted files, login records, IP addresses, malware, transaction history, browser activity and network logs. For instance, server logs can show when an intruder accessed a company database.

- **4. Interpretation.** Reconstruct what happened: how the attack occurred, which system was compromised, what was accessed, whether data was changed or stolen, and what traces remain.
- **5. Presentation in court.** Present the evidence in a legally admissible form, with experts explaining the procedure and findings.

In India, electronic records are governed by the Bharatiya Sakshya Adhiniyam, 2023. Section 63 deals with their admissibility and sets conditions for proving them. Good forensics strengthens investigations, helps establish facts and supports justice.

8. Reforms for the Road Ahead

Growing cyber threats call for a stronger framework that keeps pace with technology while protecting privacy, rights and national security. The following recommendations would help.

8.1 A comprehensive cybersecurity law

India should consider a dedicated cybersecurity statute that clearly sets out the responsibilities of government bodies, private organisations and critical infrastructure operators. It should cover prevention of attacks, incident reporting, security standards, institutional coordination, critical infrastructure protection, accountability and penalties, and international cooperation. It should also be technology-neutral, so it stays relevant as technology changes.

8.2 Sector-specific standards

One size will not fit all. Tailored standards are needed for:

- **Banking:** strong authentication, transaction monitoring and fraud protection.
- **Electricity:** security of grid-management systems and industrial control networks.
- **Telecommunications:** protection of networks and subscriber information.
- **Defence:** protection of military information and sensitive communications.
- **Healthcare:** protection of electronic medical records and hospital networks.

8.3 AI governance

India needs clearer standards for the responsible development and use of AI, including:

- **Deepfakes:** rules on creating and circulating harmful content, especially non-consensual impersonation.
- **AI-generated fraud:** legal mechanisms for AI-assisted financial fraud and identity manipulation.
- **Algorithmic accountability:** responsibility for unlawful or harmful outcomes where the law imposes it.
- **Transparency:** telling people when AI-generated or manipulated content may materially affect them.
- **Bias:** checking AI systems for discriminatory outcomes.

- **Liability:** clear allocation of responsibility among developers, deployers, operators and others, according to their conduct.

8.4 Stronger critical infrastructure protection

Critical infrastructure deserves specialised legal and technical protection: security audits, incident-reporting systems, emergency response, network monitoring, access controls, disaster recovery and public-private information sharing. Electricity, defence, telecommunications, banking and nuclear facilities need particular attention.

8.5 Building the workforce

India should invest in cybersecurity education and training, with universities offering courses in cyber law, digital forensics, ethical hacking, data protection, incident response, AI security and cryptography. Police officers, prosecutors and judges also need specialised training so they can handle technical evidence and cybercrime cases with confidence.

8.6 International cooperation

Cybercrime routinely involves people, servers and money spread across countries, so domestic enforcement alone is not enough. India should deepen cooperation on:

- Cybercrime investigation between law-enforcement agencies.
- Obtaining electronic evidence located in foreign jurisdictions.
- Sharing intelligence on threats, malware and attack methods.
- Cross-border enforcement, including jurisdiction, extradition and mutual legal assistance.
- Prosecuting offenders under applicable laws.

8.7 Balancing security and privacy

Security measures must not trample individual rights. In Justice K.S. Puttaswamy (Retd.) v. Union of India (2017), the Supreme Court affirmed that privacy is a fundamental right under Article 21 of the Constitution and an essential part of dignity, liberty and autonomy. Surveillance, data collection and cybersecurity measures must therefore stay within constitutional limits. Any restriction on privacy has to meet the applicable standards, including legality, a legitimate state purpose and proportionality. The goal is a framework that protects both the nation's digital security and individuals' fundamental rights.

9. Conclusion

Cybersecurity is now central to India's national security, economic growth and digital governance. Greater reliance on digital platforms has opened doors to growth and innovation, but it has also exposed the country to sophisticated threats. India has come a long way, through the IT Act, 2000, institutions such as CERT-In and NCIIPC, the National Cyber Security Policy, 2013 and the DPDP Act, 2023. Yet AI, deepfakes, IoT, blockchain, cloud and quantum computing raise fresh legal and technical questions, and traditional approaches to regulating cybercrime may not be enough. The analysis shows that the challenge goes well

beyond punishing offenders. It involves data protection, institutional accountability, critical infrastructure security, digital evidence, professional expertise and international cooperation. The DPDP Act and the 2025 Rules are an important step, although their main provisions will take effect in phases, and effective implementation will decide whether personal information is truly protected. India should move towards a comprehensive, adaptive and technology-neutral framework, backed by effective enforcement, specialised institutions, skilled professionals and global cooperation. Above all, regulation must balance national security, economic development, innovation and constitutional rights. The aim is not just to punish cybercrime after it happens, but to build a system of prevention, protection, detection, response, investigation and accountability.

References

Primary legal sources

- The Information Technology Act, 2000, and the Information Technology (Amendment) Act, 2008.
- The Digital Personal Data Protection Act, 2023, and the Digital Personal Data Protection Rules, 2025.
- The Bharatiya Nyaya Sanhita, 2023.
- The Bharatiya Sakshya Adhiniyam, 2023.
- The Constitution of India, 1950.
- National Cyber Security Policy, 2013.
- CERT-In Directions dated 28 April 2022, under Section 70B(6) of the IT Act, 2000.
- Japan, Basic Act on Cybersecurity, 2014.
- European Union, General Data Protection Regulation, Regulation (EU) 2016/679.
- Singapore, Personal Data Protection Act 2012.

Judicial decisions

- Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
- Shreya Singhal v. Union of India, (2015) 5 SCC 1.
- Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.
- Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.

Secondary sources

- Kartik, “An analytical study of emerging cybersecurity trends and their challenges in India,” Indian Journal of Legal Review, 2026, doi: 10.65393/ijlrv6i868.
- R. Panda, “Cybersecurity, digital governance, and national security: Emerging challenges and policy responses in India,” International Journal for Multidisciplinary Research, 2026, doi: 10.36948/ijfmr.2026.v08i04.84439.

- S. Sudhip, I. Singha and M. Atif, “Indian cyber security and defence: A comprehensive analysis,” International Journal for Research in Applied Science and Engineering Technology, 2025, doi: 10.22214/ijraset.2025.67872.
- Bheem Singh Meena, Radha Ranjan and Shyam Kumar Anand, ‘Virtual Meetings under Attack: Assessing the Legal and Security Risks of Zoom Bombing in the Digital Era’ (2023) 4(2) ShodhKosh: Journal of Visual and Performing Arts 1256–1263.
- D. Khera, “Legislation on control of cyber crime in India,” International Journal for Research in Applied Science and Engineering Technology, 2026, doi: 10.22214/ijraset.2026.79889.
- Radha Ranjan et al., ‘Policies Against Fraud and Cybercrime: Strategic, Legal, and Technological Approaches’ in Policies Against Fraud and Cybercrime: Strategic, Legal, and Technological Approaches 217–263 (IGI Global Scientific Publishing, 2026), DOI: 10.4018/979-8-3373-5992-2.ch007.
- N. Neelam, “Assessing China’s role in state-sponsored hacking: Implications for India’s national security,” Social Science Research Network, 2026, doi: 10.2139/ssrn.6392121.
- Radha Ranjan, ‘Evolution of the Doctrine of Proportionality: Assessing its Scope and Ambit in Relation to the Right to Privacy in India’ (2024) 10(1) Indian Journal of Law and Human Behavior 31–38, DOI: 10.21088/ijlhb.2454.7107.10124.3.
- Radha Ranjan and Pallavi Singh, ‘Cyber Crime Against Women in Cyberspace: A Critical Analysis of Indian Legislations’ (2023) 10(1A) Kanpur Philosopher 79–85.
- Radha Ranjan and Jivantika Gulati, ‘The Sexual Harassment against Women in Cyber Space: Concept, Reality and the Law’ (2023) 10(1) Kashmir Journal of Legal Studies.
- Aadya Misra and Mathew Chacko, “Square Pegs, Round Holes, and Indian Cybersecurity Laws,” 2(1) International Cybersecurity Law Review 57–64 (2021), DOI: 10.1365/s43439-021-00026-7.
- Annu Khan and Komal Audichya, “Cyber Security in the Indian Legal System: Challenges and a Study of Judicial Interpretation,” 5(1) Journal of Informatics Education and Research (2025), DOI: 10.52783/jier.v5i1.2153.