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

~Esita Singh

The advent of the internet has transformed India from a traditional, paper-driven bureaucracy into a global digital powerhouse. Driven by the expansion of affordable telecommunications infrastructure, digital public systems such as the Unified Payments Interface (UPI), and an exponential surge in data consumption, the nation's economic and social architecture is fundamentally digital. However, this hyper-connectivity presents significant vulnerabilities. The open, decentralized nature of cyberspace exposes critical information infrastructure, financial networks, and personal citizen data to an array of threats, including state-sponsored cyber espionage, ransomware campaigns, and systematic data exploitation.

For over two decades, India's legal framework for cyberspace relied on an adaptable but increasingly strained statutory patchwork. The foundational legal instrument, the Information Technology Act of 2000[1], was designed primarily to validate electronic commerce rather than defend against advanced, nation-state cyber warfare.[2] Over the years, the legislative landscape required structural updates. The regulatory paradigm has shifted with the enforcement of the long-awaited Digital Personal Data Protection Rules, which operationalize the landmark Digital Personal Data Protection Act of 2023. Together with stringent cyber incident reporting directives issued by the Indian Computer Emergency Response Team (CERT-In) and complementary updates to India's criminal codes, these modern frameworks represent a comprehensive legal regime governing cybersecurity, data sovereignty, and digital accountability in India.

[1] Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

[2] Enacted by the Parliament of India based on the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce adopted in 1996.

1. THE FOUNDATIONAL FRAMEWORK: THE INFORMATION TECHNOLOGY ACT, 2000

The primary legislative pillar of India's cyber law remains the Information Technology Act, 2000 (IT Act). Enacted under the shadow of the United Nations Model Law on Electronic Commerce (UNCITRAL), the original objective of the IT Act was modest: to grant legal recognition to electronic transactions, substitute digital signatures for physical executions, and facilitate e-governance.

As cyber threats mutated from simple computer tampering to systematic financial fraud and network intrusions, the gaps in the original statute became evident. This led to the passage of the Information Technology (Amendment) Act, 2008[3], which introduced extensive changes that shifted the focus toward data protection, information security, and criminal liability.

➢ CRIMINAL LIABILITY AND CYBER OFFENCES

The amended IT Act establishes a comprehensive matrix of cyber Offences and associated criminal penalties:[4]

STATUTORY ROVISIONS	NATURE OF OFFENCES	STATUTORY PENALTY
SECTION 43	Unauthorized access, data downloading, copying, or introducing viruses into a computer system.	Civil liability to pay damages by way of compensation to the affected party.
SECTION 65	Intentional tampering with, concealing, destroying, or altering computer source documents.	Imprisonment up to 3 years, or a fine up to ₹2 lakh, or both.

[3] Information Technology (Amendment) Act, 2008, No. 10, Acts of Parliament, 2009 (India).

[4] See Information Technology Act, 2000, Section.43, Section.65, Section.66, Section.66C, Section.66D, & Section.66F (as amended by Act 10 of 2009).

SECTION 66	Dishonestly or fraudulently committing any act referred to in Section 43.	Imprisonment up to 3 years, or a fine up to ₹5 lakh, or both.
SECTION 66C	Identity theft, including fraudulent use of digital signatures, passwords, or unique identification features.	Imprisonment up to 3 years, and a fine up to ₹1 lakh.
SECTION 66D	Cheating by personation by using a computer resource or communication device.	Imprisonment up to 3 years, and a fine up to ₹1 lakh.
SECTION 66F	Cyber terrorism; acts intending to threaten the unity, integrity, security, or sovereignty of India.	Imprisonment which may extend to residency for life.

- **THE CRITICAL VULNERABILITY : SECTION 43A and SECTION 72A**

The 2008 amendments introduced Section 43A and Section 72A as early attempts to address data privacy. Section 43A mandates that any body corporate possessing, handling, or dealing with Sensitive Personal Data or Information (SPDI) in a computer resource must maintain "reasonable security practices and procedures." Failure to do so resulting in wrongful loss or gain triggers a liability to pay compensation to the affected person. To implement this provision, the central government enacted the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules). [5]

While the SPDI Rules were pioneering for their time, they suffered from significant structural deficiencies:

[5] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Ministry of Communications and Information Technology, G.S.R. 313(E) (enacted April 13, 2011) (India).

- **NARROW SCOPE:** They applied exclusively to corporate entities, completely exempting state organs, government agencies, and public utilities from liability for data mismanagement.
- **DEFINITIONAL LIMITATIONS:** The category of "Sensitive Personal Data" was restricted to a rigid list (such as passwords, financial info, health conditions, and biometric data), failing to protect the broader, fluid spectrum of digital footprints generated by modern web interactions.
- **WEAK ENFORCEMENT MECHANISM:** The remedy for violations depended on state-level Adjudicating Officers, a system that lacked the specialization and institutional capacity required to tackle corporate data exploitation.

➢ SAFE HARBOR AND INTERMEDIATE LIABILITY: SECTION 79

Section 79 of the IT Act contains the "Safe Harbor" doctrine, which insulates intermediaries (such as Internet Service Providers, search engines, and social media platforms) from third-party liability. It dictates that an intermediary is not criminally or civilly liable for any third-party information, data, or communication link made available by it, provided its role is limited to providing access and it does not initiate or modify the transmission.

However, this immunity is conditional. Under Section 79(3), an intermediary must observe strict statutory "due diligence" and must expeditiously remove or disable access to illegal content upon receiving "actual knowledge" via a court order or government notification. This balance has been heavily litigated.

In the landmark decision of **Shreya Singhal v. Union of India (2015)**[6], the Supreme Court read down the phrase "actual knowledge" to mean a formal court order or an authorized directive by a government agency under Section 69A of the IT Act. This ruled out subjective "take-down requests" from private individuals, protecting free speech from private censorship.

2. EXECUTIVE SURVEILLANCE, INTERCEPTIONS, AND CONTENT BLOCKING

[6] Shreya Singhal v. Union of India, (2015) 5 S.C.C. 1 (India).

The state's authority to monitor and regulate the digital public sphere is derived primarily from Section 69 and Section 69A of the IT Act.[7] These provisions represent the intersection of national security imperatives and individual constitutional freedoms.

➢ SECTION 69: INTERCEPTION AND DECRYPTION

Section 69 empowers the central or state government to intercept, monitor, or decrypt any information generated, transmitted, received, or stored in any computer resource. To exercise this intrusive power, authorities must show that the action is necessary or expedient in the interest of: The sovereignty or integrity of India; The defense of India or security of the State; Friendly relations with foreign States; Public order; orPreventing incitement to the commission of any cognizable offence relating to the above.

This power is structured by the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.[8] These rules require formal written authorization from the Union Home Secretary or State Home Secretary, establishing a layer of senior bureaucratic review.

➢ SECTION 69A: SOVEREIGN CENSORSHIP AND CONTENT BLOCKING

Section 69A enables the government to issue directives to block public access to electronic information on grounds identical to those under Section 69. Governed by the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009[9], this provision is the legal basis for blocking foreign applications, malicious websites, and content deemed harmful to public order.

The constitutional validity of Section 69A was upheld in *Shreya Singhal v. Union of India*. The Supreme Court noted that unlike Section 66A (which the Court struck down for vagueness and

[7] See Information Technology Act, 2000, § 69 & § 69A (governing powers of interception, decryption, and public access blocking).

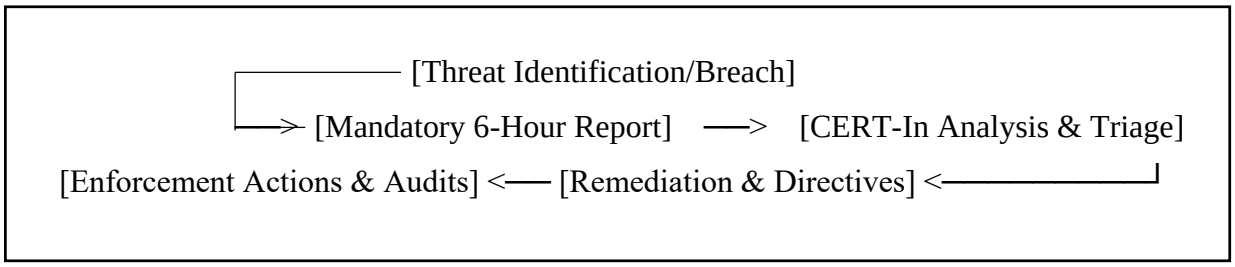
[8] Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, Ministry of Communications and Information Technology, G.S.R. 781(E) (India).

[9] Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, Ministry of Communications and Information Technology, G.S.R. 782(E) (India).

overbreadth), Section 69A contains robust procedural safeguards. These include a mandatory hearing for the affected intermediary and content creator, an explicit requirement for reasons to be recorded in writing, and oversight by an inter-ministerial review committee.

3. THE INSTITUTIONAL SENTINEL: CERT-IN AND THE 2022 CYBER SECURITY DIRECTIONS

The Indian Computer Emergency Response Team (CERT-In), established under Section 70B of the IT Act[10], serves as the national nodal agency for responding to cyber security incidents. Its responsibilities include collecting and analyzing information on cyber incidents, issuing forecasts and alerts, and coordinating emergency response measures.



In April 2022, CERT-In issued the Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 (the 2022 Directions).[11] These directives fundamentally transformed corporate compliance by introducing strict timelines and expansive logging requirements.

➢ THE 6-HOUR NOTIFICATION MANDATE

The most significant requirement of the 2022 Directions is the obligation for all service providers, intermediaries, data centers, body corporates, and government organizations to report specified cyber security incidents to CERT-In within **six hours** of noticing or being alerted to them. The covered incidents span a broad spectrum, including: Ransomware attacks and targeted malware infections; Unauthorized access to IT systems or critical infrastructure;

[10] Under Section 70B of the Information Technology Act, 2000, CERT-In operates under the Ministry of Electronics and Information Technology (MeitY).

[11] Indian Computer Emergency Response Team, Directions under sub-section (6) of section 70B of the Information Technology Act, 2000, No. 20(3)/2022-CERT-In (issued April 28, 2022) (India).

Data breaches and large-scale identity theft; Distributed Denial of Service (DDoS) attacks; and Vulnerability exploitation in critical systems.

This six-hour window is among the most aggressive regulatory reporting timelines globally, contrasting sharply with the 72-hour window found under the European Union's General Data Protection Regulation (GDPR).[12]

➢ EXPANDED LOG RETENTION OBLIGATIONS

To ensure forensic auditability during post-incident investigations, the 2022 Directions require all entities to maintain logs of their information communication systems for a rolling period of **180 days**. These logs must be stored securely within Indian territorial jurisdiction and made available to CERT-In upon request.

Furthermore, Cloud Service Providers (CSPs), Virtual Private Server (VPS) providers, and Virtual Private Network (VPN) firms are required to register and retain accurate subscriber data for a minimum of **five years** after subscription cancellation. This data includes validated customer names, physical addresses, contact details, IP addresses assigned, and ownership patterns. This requirement has caused friction with privacy-centric VPN service providers, leading some global entities to withdraw physical servers from Indian territory.

4. THE MODERN FRONTIER: THE DIGITAL PERSONAL DATA PROTECTION (DPDP) FRAMEWORK

For over a decade, India's data privacy regime was constrained by the gaps in Section 43A of the IT Act. Following the historic ruling in *Justice K.S. Puttaswamy v. Union of India* (2017)[13], where a nine-judge bench of the Supreme Court recognized the right to privacy as an intrinsic component of the Right to Life under Article 21 of the Constitution, a dedicated statutory

[12] Compare with Regulation (EU) 2016/679 (General Data Protection Regulation), Article 33, which mandates personal data breach notifications to supervisory authorities within 72 hours

[13] Justice K.S. Puttaswamy v. Union of India, (2017) 10 S.C.C. 1 (India). 14 Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

overhaul became necessary. This resulted in the enactment of the Digital Personal Data Protection Act, 2023 (DPDP Act) on August 11, 2023.[14]

The framework has advanced to operational enforcement with the notification of the Digital Personal Data Protection Rules, 2025.[15] Together, the Act and its rules establish a citizen-centric compliance regime designed to secure individual privacy without impeding digital innovation.

➢ SCOPEAND EXTRATERRITORIAL APPLICATION

The DPDP Act governs the processing of "digital personal data" within India, including data collected digitally or gathered offline and subsequently digitized.

Crucially, Section 3(b) grants the Act **extraterritorial reach**. It applies to the processing of digital personal data outside the territory of India if such processing is in connection with any activity related to offering goods or services to Data Principals within India. For instance, a foreign-based SaaS platform or an e-commerce enterprise processing data belonging to residents within India must strictly comply with the DPDP framework.

➢ THE COMPLIANCE TRIAD: PRINCIPALS, FIDUCARIES, AND PROCESSORS

The statute replaces traditional Western nomenclature (such as "data subject" and "data controller") with terms tailored to Indian jurisprudence:

- **DATA PRINCIPAL:** The individual to whom the personal data relates. Where the individual is a child or a person with a disability, the term encompasses their parents or lawful guardians.
- **DATA FIDUCIARIES:** Any person or entity who, alone or in conjunction with others, determines the purpose and means of the processing of personal data.
- **DATA PROCESSORS:** Any person or entity who processes personal data on behalf of a Data Fiduciary.

➢ CORE LEGAL BASES FOR DATA PROCESSING

[14] Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

[15] Digital Personal Data Protection Rules, 2025, Ministry of Electronics and Information Technology, G.S.R. Gazette Notification (notified Nov. 13, 2025) (India).

Under Section 4, data processing is permissible only if it adheres to a lawful basis. The framework establishes two explicit pillars for processing:

1. **CONSENT:** Consent must be free, specific, informed, unconditional, and unambiguous, requiring a clear affirmative action from the Data Principal. The request for consent must be accompanied or preceded by a granular, easy-to-understand privacy notice available in English or any of the 22 languages listed in the Eighth Schedule to the Indian Constitution.[16]
2. **LEGITIMATE USES:** Section 7 identifies specific scenarios where data can be processed without explicit consent. These include voluntary data sharing by the principal for a specific purpose, processing for state security or public order, responding to medical emergencies, fulfilling legal obligations, or managing corporate employment relationships.

➢ CODIFICATION OF PRIVACY PRINCIPLES

The architecture of the DPDP Act explicitly incorporates foundational privacy principles:

DPDP Core Principles:
1. Purpose Limitation (Process only for stated goals)
2. Data Minimization (Collect only what is necessary)
3. Storage Limitation (Delete when purpose is served)
4. Accuracy & Integrity (Maintain precise records)

- **PURPOSE LIMITATIONS:** Data Fiduciaries can process data only for the precise purpose specified in the notice provided to the Data Principal.
- **DATA MINIMIZATION:** Fiduciaries are restricted from collecting excessive information beyond what is strictly necessary to achieve the stated purpose.
- **STORAGE LIMITATION:** Once the specified purpose is fulfilled or consent is withdrawn, the Data Fiduciary must delete the data and direct its Data Processors to do the same.

➢ THE TIERED ENFORCEMENT SCHEDULE UNDER THE 2025 RULES

[16] Constitution of India, Eighth Schedule (listing the 22 official regional languages recognized in India.

The Digital Personal Data Protection Rules, 2025, outline a structured, phased implementation schedule designed to allow enterprises to transition into compliance without causing systemic economic disruption:[17]

- **STAGE 1 (IMMEDIATE):** Establishment of the Data Protection Board of India (DPBI) along with its procedural operational rules.
- **STAGE 2 (12-MONTH MILESTONE):** Implementation of the formal mechanism for the registration and regulation of *Consent Managers*—specialized interoperable platforms that empower Data Principals to give, manage, review, and revoke consent through a single digital interface.[18]
- **STAGE 3 (18-MONTH MILESTONE):** Full enforcement of core compliance mandates. This includes mandatory privacy disclosures, systemic security protocols, automated data breach notification mechanisms, specific protections for children's data, and specialized rules for Significant Data Fiduciaries (SDFs).

➢ SIGNIFICANT DATA FIDUCIARIES (SDFs)

The central government can designate certain entities as Significant Data Fiduciaries based on factors like the volume of data processed, potential risks to the sovereignty of India, or impacts on public order. SDFs face heightened compliance requirements, including the mandatory appointment of a resident Data Protection Officer (DPO), independent statutory data audits, and regular Data Protection Impact Assessments (DPIAs).

➢ FINANCIAL PENALITIES AND ENFORCEMENT ARCHITECTURE

The DPDP Act removes provisions for criminal imprisonment for privacy infractions, choosing instead to enforce a stringent civil penalty regime. The Data Protection Board of India (DPBI) functions as a specialized quasi-judicial body empowered to investigate data breaches, adjudicate disputes, and levy penalties based on the severity of the violation:

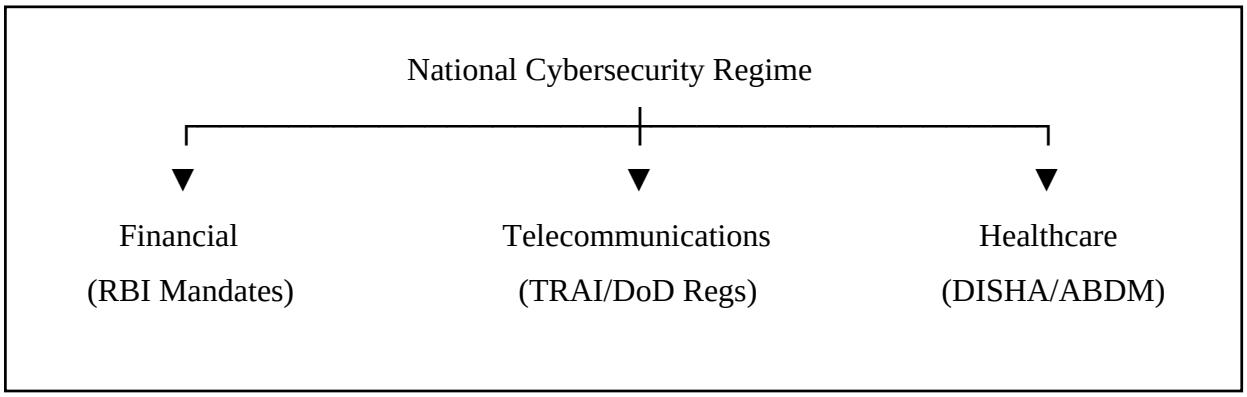
[17] Digital Personal Data Protection Act, 2023, § 8 & § 9 (detailing specific responsibilities regarding accuracy, data breach notifications, and strict prohibitions on tracking children's data).

[18] Digital Personal Data Protection Rules, 2025, Rule 4 & Rule 7 (operationalizing the phased transition and consent manager framework).

- Failure to implement reasonable technical and organizational measures to prevent data breaches: Up to ₹250 crore.
- Failure to notify the DPBI or affected Data Principals of a personal data breach: Up to ₹200 crore.
- Violation of specialized processing obligations concerning children's personal data: Up to ₹200 crore.

5. SECTORAL REGULATIONS AND CRITICAL INFRASTRUCTURE PROTECTION

Beyond overarching statutes like the IT Act and the DPDP framework, specialized sectors operate under distinct cybersecurity regulations managed by their respective statutory regulators.



➢ THE FINANCIAL SECTOR: RESERVE BANK OF INDIA (RBI) DIRECTIVES

The RBI maintains a strict regulatory posture regarding electronic banking and fintech security. Its frameworks require commercial banks, Non-Banking Financial Companies (NBFCs), and payment aggregators to implement comprehensive cyber security architectures. Key mandates include:

- **DATA LOCALIZATION:** Under the 2018 storage of payment system data directive, all payment system providers must ensure that the entire data relating to payment systems

operated by them is stored in a system located only in India.[19] This includes end-to-end transaction details, credentials, and customer information.

- **ADVANCED SECURITY CONTROLS:** Financial institutions must deploy continuous automated vulnerability scanning, multi-factor authentication (MFA) for all remote sessions, secure application programming interfaces (APIs), and real-time fraud monitoring systems.
- **CYBER INCIDENT REPORTING:** Separate from CERT-In timelines, regulated financial entities must report any cyber security event to the RBI's Cyber Security and Information Technology Examination (CSITE) cell within **2 hours** of detection.[20]

➢ CRITICAL INFORMATION INFRASTRUCTURE: NCIIPC

Section 70 of the IT Act governs Critical Information Infrastructure (CII)[21], defined as any computer resource whose destruction or incapacitation would have a debilitating impact on national security, economy, public health, or safety. The National Critical Information Infrastructure Protection Centre (NCIIPC) serves as the designated national agency for securing these installations.[22] It categorizes critical sectors into distinct verticals:

1. Power and Energy,
2. Banking, Financial Services & Insurance (BFSI),
3. Telecom and Information Technology,
4. Transport (Railways, Aviation, Maritime),
5. Strategic and Government Enterprises, and
6. Core Public Utilities.

[19] Reserve Bank of India, Directive on Storage of Payment System Data, DPSS.CO.OD No. 2785/06.08.005/2017-18 (issued April 6, 2018) (India).

[20] Cyber Security and Information Technology Examination (CSITE) Cell, Department of Supervision, Reserve Bank of India.

[21] Information Technology Act, 2000, § 70 (empowering the state to declare any computer resource as a protected system).

[22] The National Critical Information Infrastructure Protection Centre (NCIIPC) was formally established via Gazette Notification on January 16, 2014, operating as a unit under the National Technical Research Organisation (NTRO).

NCIIPC mandates specific defense mechanisms for these assets, including physical air-gapping of Operational Technology (OT) from corporate Information Technology (IT) networks, mandatory deployment of indigenous hardware components, regular cyber-warfare simulation drills, and continuous security operations center (SOC) monitoring.

6. THE INTERSECTION OF CYBERSECURITY AND CRIMINAL LAW

The prosecution of cybercrime in India has been updated by replacing colonial-era criminal statutes with modernized codes: the Bharatiya Nyaya Sanhita, 2023 (BNS)[23], which replaces the Indian Penal Code, 1860 (IPC); and the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS)[24], which replaces the Code of Criminal Procedure, 1973 (CrPC).

➢ SUBSTANTIVE ALIGNMENT: THE BNS

The BNS updates definitions of traditional crimes to fully encompass digital mediums. Offences like extortion, cheating, forgery, and criminal intimidation now explicitly cover actions executed via computer resources, digital communication networks, or encrypted platforms. Furthermore, provisions addressing organized crime syndicate operations account for digital theft, online betting scams, and systemic digital financial frauds.

➢ ADMISSIBILITY OF ELECTRONIC EVIDENCE: THE BSB and BNSS

The Bharatiya Sakshya Bill, 2023 (BSB)[25], which replaces the Indian Evidence Act, 1872, revises the admissibility criteria for electronic records. It recognizes digital assets—including smartphone data, cloud records, server logs, metadata, and encrypted chat histories—as primary documentary evidence.

To preserve the chain of custody and prevent tampering during digital forensics investigations, Section 105 of the BNSS mandates that search and seizure operations conducted by law enforcement agencies, including the confiscation of electronic devices like laptops or

[23] Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023 (India) (repealing and replacing the Indian Penal Code, 1860).

[24] Bharatiya Nagarik Suraksha Sanhita, 2023, No. 46, Acts of Parliament, 2023 (India) (repealing and replacing the Code of Criminal Procedure, 1973).

[25] Bharatiya Sakshya Bill, 2023, No. 47, Acts of Parliament, 2023 (India) (repealing and replacing the Indian Evidence Act, 1872).

smartphones, **must be audio-video recorded**. This recorded digital footprint must be submitted to the jurisdictional magistrate without delay to verify the integrity of the collected digital evidence.

7. COMPARATIVE ANALYSIS: INDIA'S FRAMEWORK vs. INTERNATIONAL STANDARDS

India's evolving cybersecurity and data privacy matrix represents a hybrid model that balances European rights-focused principles with American market-driven innovations.

LEGAL/REGULATORY DIMENSIONS	INDIA (IT ACT + DPDP ACT + CERT-IN)	EUROPEAN UNION (GDPR + NIS2)	UNITED STATES (FTC + CCPA + CISA)
PRIMARY STATUTORY BASIS	IT Act, 2000; DPDP Act, 2023.	General Data Protection Regulation (GDPR); NIS2 Directive.[26]	Fragmented: Sectoral federal laws (HIPAA, GLBA) + State laws (CCPA/CPRA).
EXTRATERRITORIAL REACH	Yes, if offering goods/services to individuals within India.	Yes, if targeting EU residents or monitoring their behavior.	Varied; state-level statutes apply to businesses targeting state residents.
BREACH NOTIFICATION TIMELINE	**6 Hours** for cyber security incidents to CERT-In.	**72 Hours** for personal data breaches to Supervisory Authorities.	Varied; typically 30–60 days under state laws; 72 hours for

[26] NIS2 Directive (Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union).

			critical infrastructure under CIRCIA.[27]
FINANCIAL PENALTIES	Up to ₹250 crore (~$30M USD) per infraction; no criminal terms for privacy.	Up to €20 million or 4% of global annual turnover, whichever is highe.	Varied state statutory fines; up to $50,000+ per deliberate violation under CCPA.[28]
DATA LOCALIZATION REQUIREMENTS	Conditional: Sectoral mandates (RBI) require strict financial localization.	Restricted cross-border transfer unless adequacy status or SCCs exist.	Generally open cross-border flows, subject to national security reviews (CFIUS).

8. CURRENT CHALLENGES AND FUTURE TRAJECTORIES

Despite recent statutory progress, India's cybersecurity landscape faces several systemic operational, legal, and structural challenges:

➢ HARMONIZING OVERLAPPING JURISDICTIONS

An immediate challenge is the institutional overlap between CERT-In and the Data Protection Board of India (DPBI). If an enterprise suffers a ransomware attack that compromises personal data, it faces two separate reporting requirements: notifying CERT-In within 6 hours under the 2022 Directions, and notifying the DPBI of the data breach under the DPDP framework.

[27] Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), 6 U.S.C. §§ 681–681g (United States).

[28] California Consumer Privacy Act of 2018 (CCPA), Cal. Civ. Code §§ 1798.100 et seq., amended by the California Privacy Rights Act of 2020 (CPRA).

Resolving inconsistencies between these reporting timelines and coordinating investigations between the two bodies remains a pressing regulatory issue.

➢ MANAGING STATE EXEMPTIONS

Section 12 of the DPDP Act allows the central government to exempt any state instrumentality from the core provisions of the Act in the interest of national sovereignty, state security, or public order.[29] Legal experts and civil rights groups note that without independent judicial oversight, broad government exemptions could weaken data protection standards, potentially complicating international data transfer adequacy agreements with jurisdictions like the European Union.

➢ CAPACITY AND SPECIALISED SKILLS SCARCITY

The effectiveness of India's updated legal frameworks depends on the technical capacity of its enforcement agencies. Law enforcement personnel often lack advanced digital forensics training, which can lead to procedural errors during device data seizures. Similarly, the judiciary faces backlogs in resolving complex cyber disputes, highlighting the need for specialized cyber courts and continuous technical education for judicial officers.

9. CONCLUSION

India has established a structured cybersecurity architecture that transitions its legal framework from a reactive stance to a proactive compliance regime. The combination of the Information Technology Act, the phased enforcement of the Digital Personal Data Protection Rules, and targeted sectoral directives from institutions like the RBI and NCIIPC forms a comprehensive regulatory framework.

As India's digital economy expands, the success of its cybersecurity strategy will depend on execution. Achieving this requires balancing economic innovation with individual privacy rights, resolving institutional jurisdiction overlaps, and building technical capacity across law enforcement and judicial bodies. By addressing these structural challenges, India can protect

[29] Digital Personal Data Protection Act, 2023, § 12 (empowering the Central Government to exempt state instrumentalities via notification).

its critical information infrastructure, secure its digital public goods, and establish a resilient framework for its digital future.

REFERENCES

- Bharatiya Nagarik Suraksha Sanhita, 2023, No. 46, Acts of Parliament, 2023 (India).
- Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023 (India).
- Bharatiya Sakshya Bill, 2023, No. 47, Acts of Parliament, 2023 (India).
- Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
- Digital Personal Data Protection Rules, 2025, Ministry of Electronics and Information Technology, G.S.R. Gazette Notification (notified Nov. 13, 2025) (India).
- Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
- Information Technology (Amendment) Act, 2008, No. 10, Acts of Parliament, 2009 (India).
- Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Ministry of Communications and Information Technology, G.S.R. 313(E) (enacted April 13, 2011) (India).
- Indian Computer Emergency Response Team, Directions under sub-section (6) of section 70B of the Information Technology Act, 2000, No. 20(3)/2022-CERT-In (issued April 28, 2022) (India).
- Justice K.S. Puttaswamy v. Union of India, (2017) 10 S.C.C. 1 (India).
- Reserve Bank of India, Directive on Storage of Payment System Data, DPSS.CO.OD No. 2785/06.08.005/2017-18 (issued April 6, 2018) (India).
- Shreya Singhal v. Union of India, (2015) 5 S.C.C. 1 (India).