IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

The Expanding Contours Of Corporate Liability In Cybercrime

FIRST AUTHOR- DIVYA

LL.M. (Master of Laws), UILS, Chandigarh University

SECOND AUTHOR- Dr Amrita Rathi

Associate Professor, UILS, Chandigarh University

Abstract

Corporate liability for cybercrimes in India has moved from a narrow focus on individual wrongdoers to a wider scrutiny of organisational systems, board oversight, digital supply chains, and technology partners. This shift became sharper after the "Indian Computer Emergency Response Team (CERT-In) Directions dated 28 April 2022" imposed a six-hour reporting window, uniform time synchronisation, and log retention for a large class of service providers and corporate entities, since any silence or delay now points directly to organisational default rather than to a faceless attacker. At the same time, the "Digital Personal Data Protection Act, 2023" created an administrative penalty regime of up to INR 250 crore for failure to take reasonable security safeguards, thereby converting many data compromise situations from a criminal pursuit to a regulatory and quasi-civil exposure that still sits side by side with the criminal offences in the "Information Technology Act, 2000" and allied laws. The study explores how "Section 85 of the Information Technology Act, 2000" builds vicarious liability on persons in charge, how "Section 79 of the Information Technology Act, 2000" retains conditional immunity for intermediaries, how the 2021 Intermediary Rules as updated on 6 April 2023 expand due diligence, and how the new criminal codes, mainly the "Bharatiya Nyaya Sanhita, 2023" and the "Bharatiya Sakshya Adhiniyam, 2023", supply the general criminal law backdrop for corporate cyber prosecutions after 1 July 2024. The paper reads these instruments together with leading rulings such as "*Standard Chartered Bank v. Directorate of Enforcement*", "*Iridium India Telecom Ltd v. Motorola Inc.*", and "*Shreya Singhal v. Union of India*" to show that Indian courts are ready to attach mens rea to juristic persons, to pierce managerial layers, and to deny safe harbour where platform conduct becomes active. The analysis culminates in governance-oriented suggestions and a harmonised view of corporate-facing duties across IT Act, CERT-In, DPDP, and BNS regimes.

Keywords: corporate liability; cybercrimes; Section 85 IT Act; intermediary liability; DPDP Act 2023; CERT-In; BNS 2023; due diligence; governance; jurisprudence

1.1 INTRODUCTION

The growth of digital markets, platform-based delivery services, managed cloud hosting, and fintech models in India has brought unprecedented exposure to cyber offences that were earlier counted as sporadic economic offences. After the 2022 CERT-In directions, most medium and large Indian companies now operate under a regime where a ransomware strike, an insider enabled data theft, or a credential stuffing attack on customer wallets becomes a reportable event within hours, else the non-reporting itself forms a contravention of directions issued under "Section 70B(6) of the Information Technology Act, 2000". Such non-reporting is easy to prove from server logs and CERT-In's own time stamps, which sharply increases prosecutorial leverage over corporate bodies and over those officers who were responsible for maintaining records. The DPDP Act, 2023, notified on 11 August 2023 and operationalised through the Data Protection Board, runs in parallel and looks at the same events from the angle of personal data breach, making the same senior personnel answerable for choice of processors, vetting of contracts, and timely breach notification.[1]

This convergence of cyber incident reporting, data protection, and platform due diligence arrives at a time when Indian criminal law itself has been recast through the "Bharatiya Nyaya Sanhita, 2023", the "Bharatiya Nagarik Suraksha Sanhita, 2023", and the "Bharatiya Sakshya Adhiniyam, 2023", which came into force on 1 July 2024 and replaced the IPC, CrPC, and Evidence Act. These codes were not written exclusively for cyber offences, yet they contain distinct clauses on organised crime, cheating, or personation using computer resources, and they strengthen electronic evidence presumptions, thereby allowing cyber prosecutions to be run under BNS and BNSS while keeping IT Act specific offences alive. For companies this means that an offence committed through a computer system can be charged in two tracks, one under the special law and another under the general code, and withdrawal of one charge does not dilute the other. Such dual exposure is important because many boardrooms still treat the IT Act as an economic legislation and underestimate the prison facing parts of BNS that now sit behind cyber frauds, data exfiltration rings, and platform-mediated contraband sales.[2]

A second feature of the current techno legal setting is the growing weight placed on intermediary compliance. The 2021 Intermediary Guidelines and Digital Media Ethics Code Rules, read with the 2022 and 2023 amendments, require almost every significant online service to appoint key officers in India, to preserve data for law enforcement, to respond to government or court orders within specified hours, and to act on user grievances through a visible mechanism. Non-compliance erodes the safe harbour offered by "Section 79 of the Information Technology Act, 2000", which in turn exposes the platform to claims and criminal investigations for user generated harms. The coming draft regime on synthetically generated information in

[1] Directions Under Sub-Section (6) of Section 70B of the Information Technology Act, 2000 Relating to Information Security Practices, Procedure, Prevention, Response and Reporting of Cyber Incidents for Safe & Trusted Internet, *available at:* https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf (last visited on October 31, 2025).

[2] New Criminal Laws to Be Effective From 1st July 2024, *available at:* https://www.cyberpeace.org/resources/blogs/new-criminal-laws-to-be-effective-from-1st-july-2024 (last visited on October 30, 2025).

2025, which builds on the same rules, shows that the Government continues to read the safe harbour as a conditional shield that can be narrowed through subordinate legislation whenever new cyber harms surface.[3] The third strand is enforcement energy. From 2022 onwards law enforcement agencies, sectoral regulators, and the Data Protection Board's preparatory secretariat have all moved towards early seizure of logs, insistence on precise time stamps, and cross referencing with telecom or cloud service providers. The BNSS requires forensic investigation in offences punishable with seven years or more, which fits neatly with complex cyber frauds and coordinated ransomware cases, since electronic evidence collected through BNSS and admitted through BSA gives the prosecution a much cleaner evidentiary path than before. Corporate defendants now have to demonstrate that they put in place reasonable security practices, complied with CERT-In, ran grievance and takedown processes, and escalated incidents swiftly, or else the presumption tilts against them even before mens rea is argued.[4]

1.2 STATUTORY FRAMEWORK

Corporate liability for cybercrimes in India does not arise from a single enactment but from a mesh of primary statutes, subordinate rules, and executive directions that often attach liability both to the corporate person and to those responsible for the conduct of its business. The IT Act, 2000, being the earliest code, laid down offences and also shielded intermediaries, but the rise of platform business models, high velocity user generated content, and deep digital supply chains required later instruments to press harder on corporate bodies. The 2022 CERT-In directions introduced highly specific operational obligations for entities that were not necessarily framed as accused persons, yet disobedience to those directions is traceable back to the parent Act. The DPDP Act, 2023 completed this move by treating failure to maintain reasonable security safeguards or to notify breaches as wrongs that attract steep monetary penalties instead of only criminal prosecution, but these civil consequences still feed into criminal prosecutions where wilful neglect is shown. The BNS, BNSS, and BSA, together effective from July 2024, now supply the general provisions on attempt, abetment, conspiracy, organised crime, and admissibility of electronic evidence which are used whenever the IT Act alone does not provide a complete prosecutorial route.[5]

1.2.1 Information Technology Act 2000

The IT Act, 2000 continues to be the central statute for cyber offences and corporate exposure. "Section 85 of the Information Technology Act, 2000" states that where a contravention has been committed by a company, every person who at the time of the contravention was in charge of and responsible to the company for the conduct of the business, as well as the company, shall be guilty and liable to be proceeded against and punished, provided that such person can escape liability by proving that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention. The section clarifies that

[3] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 [Updated as on 6.4.2023], *available at:* https://www.meity.gov.in/static/uploads/2024/02/Information-Technology-Intermediary-Guidelines-and-Digital-Media-Ethics-Code-Rules-2021-updated-06.04.2023-.pdf (last visited on October 29, 2025).

[4] The Bharatiya Nagarik Suraksha Sanhita, 2023, *available at:* https://prsindia.org/billtrack/the-bharatiya-nagarik-suraksha-sanhita-2023 (last visited on October 28, 2025).

[5] The Information Technology Act, 2000, *available at:* https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf (last visited on October 27, 2025).

the word company includes body corporate, firm, or association of individuals, and that director in relation to a firm means a partner, which widens the net far beyond listed companies. This creates a statutory presumption of joint guilt that reverses the usual burden in criminal law and places on the officer the duty to show positive preventive steps such as cyber security policies, access controls, or reporting mechanisms. The structure is important because it makes non observance of CERT-In directions, non-cooperation with agencies, or non-maintenance of reasonable security practices not only a corporate default but also an individual offence.[6]

1.2.2 Intermediary Safe Harbour

"Section 79 of the Information Technology Act, 2000" gives intermediaries exemption from liability for third party information, data, or communication link made available or hosted by them, provided that the function is limited to providing access to a communication system and that the intermediary observes due diligence and also complies with government prescribed guidelines. This safe harbour is not absolute, because "Section 79(3)" takes it away where the intermediary has conspired, abetted, or aided in the commission of an unlawful act, or upon receiving actual knowledge through a court order or government notification fails to expeditiously remove or disable access to the material. The 2021 Rules read with the April 2023 update make this due diligence concrete through obligations relating to user agreements, takedown procedures, appointment of compliance officers, 24-hour acknowledgement and 15-day disposal of grievances, and 72-hour response to law enforcement queries. Intermediaries that step beyond a passive conduit role, such as by ranking, promoting, or monetising content, risk being treated as active participants and therefore losing safe harbour.[7]

1.2.3 CERT-In Directions 2022

The directions issued on 28 April 2022 under "Section 70B(6) of the Information Technology Act, 2000" require service providers, intermediaries, data centres, corporate bodies, and Government organisations to report prescribed cyber incidents to CERT-In within six hours of noticing such incidents or being notified of such incidents, to synchronise their ICT system clocks to the Network Time Protocol of the National Informatics Centre or National Physical Laboratory, to enable logs of all ICT systems and maintain them securely for a rolling period of 180 days within Indian jurisdiction, and to provide handover of logs and digital evidence to CERT-In when directed. The directions are drafted in mandatory language and mention that failure to furnish the required information may invite action under the IT Act. For corporate entities this creates a new class of offences by omission, because a ransomware victim who restores operations quietly or an online marketplace that deletes rogue content but does not file a report may still face prosecution under "Section 85" read with the directions.

[6] Section 85 - The Information Technology Act, *available at:* https://lawgist.in/information-technology-act/85 (last visited on October 26, 2025).

[7] Anirudh Rastogi, *Cyber Law: Law of Information Technology and Internet* 130 (LexisNexis, New Delhi, 1st edn., 2014).

1.2.4 DPDP Act 2023

The "Digital Personal Data Protection Act, 2023" altered the accountability calculus by introducing a Board driven inquiry and penalty model in which the Data Protection Board can, after finding non-compliance with security safeguards or breach notification requirements, impose monetary penalties that go up to INR 250 crore for the most serious violations such as failure to take security measures to prevent a personal data breach or failure to protect children's data. The Act treats companies as data fiduciaries and, for certain volumes or risk classes, as significant data fiduciaries, and therefore expects them to appoint a Data Protection Officer, to publish contact details, to conduct data protection impact assessments, and to notify the Board and affected data principals in the event of a personal data breach. While the Act is mainly civil regulatory in design and does not usually turn every breach into a criminal offence, the high ceiling of the penalty and the statutory requirement to coordinate with CERT-In and other sectoral regulators create strong incentives for boards to show that they had exercised due diligence in line with "Section 85 of the IT Act, 2000". The Act also serves as a benchmark for measuring carelessness, so gaps noted by the Board may later be used in criminal proceedings to argue consent, connivance, or neglect by responsible persons.[8]

1.2.5 BNS 2023 Interface

The "Bharatiya Nyaya Sanhita, 2023" supplies several offence heads that can be read with the IT Act to prosecute cybercriminal conduct that originates from or is enabled by corporate structures. Provisions on organised crime, cheating, breach of trust, and forged electronic records can now be applied to situations where business managers knowingly permit the corporate platform to be used for phishing campaigns, money laundering through mule accounts, or sale of restricted items, and "Section 336 of the Bharatiya Nyaya Sanhita, 2023" in particular captures cheating through online or digital means similar to the earlier practice under IPC sections dealing with cheating by personation. Where insiders siphon digital assets or manipulate vendor payments, the cheating or criminal breach of trust provisions of BNS can run in parallel with "Sections 66C and 66D of the IT Act, 2000" as they were retained for identity theft and cheating by personation using computer resources. BNSS, 2023 strengthens this by requiring forensic investigation for serious offences and by enabling digital serving of summons and digital recording of search and seizure, which makes it easier to gather board minutes, dashboards, email trails, and cloud logs against the company and its key functionaries. The "Bharatiya Sakshya Adhiniyam, 2023" recognises electronic records as documents and eases admission where the conditions for computer output are met, which removes earlier evidentiary objections that used to help corporate accused.[9]

1.3 INTERMEDIARY LIABILITY AND PLATFORM GOVERNANCE

Intermediary liability sits at the heart of corporate exposure for cybercrimes because a very large number of Indian offences today are committed through user generated content, anonymous handles, online marketplace listings, and messaging channels operated by companies that do not themselves author the harmful content.

[8] Rahul Matthan, *Privacy 3.0: Unlocking Our Data-Driven Future* 210 (HarperCollins, Gurugram, 1st edn., 2020).

Indian law chose to give such intermediaries a conditional safe harbour but surrounded it with detailed procedural and technical duties, so that an intermediary that actively curates content, monetises it, or refuses to respond to lawful orders can be treated as having participated in the offence. The reading down of "Section 79 of the IT Act, 2000" by the Supreme Court in 2015 limited the Government's ability to order takedowns without prior judicial or executive process, yet it did not dismantle the due diligence framework, which was later expanded in 2021, 2022, 2023, and now in 2025 draft amendments dealing with synthetically generated information. This area is especially important for corporate liability because officers of intermediaries can be summoned and prosecuted when safe harbour is lost.[10]

1.3.1 Shreya Singhal v. Union of India

In the case of "*Shreya Singhal v. Union of India*[11], a two-judge bench of the Supreme Court considered a batch of writ petitions challenging the constitutionality of several provisions of the IT Act and the Rules, mainly on the ground that they violated the right to freedom of speech and expression under Article 19(1)(a) of the Constitution. The Court struck down "Section 66A of the Information Technology Act, 2000" in its entirety because the expressions used in the section, such as grossly offensive, menacing, or causing annoyance or inconvenience, were vague, overbroad, and not saved by any of the grounds under Article 19(2). While doing so, the Court recognised the special reach and power of the internet and refused to accept government assurances that the provision would be used with restraint, holding that such assurances could not cure an unconstitutional statute. This part of the judgment is widely known, but for the present study the more relevant portion is where the Court read down "Section 79" and Rule 3(4) of the 2011 Intermediary Guidelines. The Court held that intermediaries could not be compelled to remove content on the basis of private complaints alone, and that the obligation to remove or disable access to information would arise only when the intermediary received a court order or a notification from the Government or its agency. This reading preserved safe harbour by preventing a flood of private takedown demands and by tying intermediary liability to formal knowledge.

The Court in "Shreya Singhal" also upheld the blocking power under "Section 69A of the IT Act, 2000" as constitutionally valid because it was narrowly drawn and contained procedural safeguards such as opportunity of hearing, reasoned order, and review committee. By distinguishing between an overbroad criminal speech offence and a targeted blocking provision, the Court signalled that intermediary obligations that arise from clear statutory or rule-based procedures would survive constitutional scrutiny. This part of the judgment has made it easier for the Government to expand intermediary due diligence through the 2021 Rules and subsequent amendments, and to insist on quick turnaround for law enforcement requests, because such obligations are viewed as extensions of a constitutionally approved framework. For corporate intermediaries, the case therefore has a dual effect: it guards them against arbitrary content removal demands that bypass due process, yet it also tells them that once a lawful order is served or once actual knowledge is received, failure to act will lead to loss of safe harbour and potential criminal prosecution. The Court's

[10] Shreya Singhal vs U.O.I on 24 March, 2015, *available at:* https://indiankanoon.org/doc/110813550/ (last visited on November 1, 2025).
[11] (2015) 5 SCC 1.

approach also opened the door for more nuanced obligations, such as traceability for significant social media intermediaries, transparency reporting, and now labelling of synthetically generated information, all of which can be justified as procedural conditions to enjoy the statutory immunity granted by "Section 79".[12]

1.3.2 Intermediary Rules as Amended 2023

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as updated on 6 April 2023, impose a comprehensive due diligence regime on intermediaries of all sizes and a stricter one on significant social media intermediaries. They require intermediaries to publish rules and regulations, privacy policy, and user agreement; to inform users not to host, display, upload, modify, publish, transmit, store, update, or share prohibited content; to appoint a Grievance Officer, a Nodal Contact Person, and a Chief Compliance Officer resident in India for significant platforms; to acknowledge user complaints within 24 hours and resolve them within 15 days; to remove or disable access to content within 24 hours in cases involving sexual material or impersonation; to preserve content and associated records for 180 days or longer when directed; and to provide information under their control to law enforcement agencies within 72 hours. The 2023 update brought online gaming and fact checking advisories into the frame and signalled that intermediaries are expected to carry out periodic risk assessments. These rules operate as the practical benchmark for determining whether an intermediary observed due diligence under "Section 79(2)(c)". Failure to follow them converts what would have been a shield into an aggravating factor in cybercrime prosecutions.[13]

1.3.3 Safe Harbour Stress Points

Safe harbour in India now faces three clear stress points. The first arises from non-compliance with due diligence requirements under the 2021 Rules as amended, which allows regulators and complainants to argue that the intermediary did not qualify for "Section 79" protection in the first place. The second arises after receipt of actual knowledge in the form of a court order or government notice, where failure to act with speed or to preserve evidence directly attracts "Section 79(3)" and, in serious matters, directions under "Section 70B(6)" for cooperation. The third stress point is the shift in policy thinking seen in 2024-2025 consultations on the Digital India Act and on amendments to the IT Rules, which seek to regulate synthetically generated information, deepfakes, and high-risk AI tools by imposing proactive detection, labelling, and user verification duties on platforms. Each of these proactive duties moves the intermediary one step away from being a mere conduit and therefore makes courts more willing to see knowledge, control, or inducement in the intermediary's conduct, narrowing safe harbour. Companies that do not maintain well documented grievance redressal processes, incident response playbooks, and AI content labelling systems will find it difficult to prove due diligence when charged for user generated cyber offences.[14]

[12] Chinmayi Arun, "Gatekeeper Liability and Article 19(1)(a) of the Constitution", 7 *NUJS Law Review* 15 (2014).
[13] Pavan Duggal, *Cyber Law* 160 (Universal Law Publishing, New Delhi, 1st edn., 2016).
[14] Decoding the Proposed IT Amendment Rules, 2025, *available at:* https://theleaflet.in/digital-rights/law-and-technology/decoding-the-proposed-it-amendment-rules-2025 (last visited on October 31, 2025).

1.4 ENFORCEMENT AND INCIDENT TRENDS

Indian corporate actors now face a layered enforcement space in which technical regulators, data protection authorities, and regular criminal law agencies all move on the same factual incident, creating a composite exposure that did not exist when cyber incidents were treated largely as IT department issues. The 2022 directions under "Section 70B of the Information Technology Act, 2000" brought CERT-In from an advisory role into a quasi-forensic gatekeeper, because the six-hour intimation requirement, log retention for 180 days within India, and power to seek real-time traffic data mean that even tentative events immediately create documentary trails that compliance teams cannot later rewrite. Parallelly, the "Digital Personal Data Protection Act, 2023" brought a schedule-led penalty model and empowered the Data Protection Board to open inquiries on its own motion, so a single ransomware event or credential stuffing attack may generate at least two statutory processes plus any BNS-based FIR that police may register for cheating, identity theft or organised crime. The common thread is that every one of these laws speaks in terms of responsibility of the person in charge, allowing prosecutors to reach management through "Section 85 of the Information Technology Act, 2000" when procedural lapses are traceable to human decisions.[15]

1.4.1 CERT-In Reporting and Audits

The six-hour reporting window is short enough to force corporations to treat detection, triage, and regulatory disclosure as a single workflow, not three distinct stages, because the 2022 directions require reporting of a wide list of incidents including targeted scanning, compromise of critical systems, data leaks, and attacks on cloud resources, even when the internal investigation is still gathering facts. These directions require service providers, intermediaries, data centres, and all bodies corporate to sync their clocks to an approved time source and to keep all ICT system logs within India for 180 days, so during BNSS-governed investigations the police can demand the same historic logs that were earlier supplied to CERT-In, and those logs will usually meet "Sections 61 to 63 of the Bharatiya Sakshya Adhiniyam, 2023" on admissibility of electronic records, closing one more escape route. Because the directions also authorise CERT-In to seek additional information and issue orders to redress vulnerabilities, every follow-up e-mail or portal upload becomes a traceable event that can be contrasted with what the board or CISO told shareholders or auditors, enabling charge sheets to plead concealment or negligence against natural persons.[16]

1.4.2 Sample Police Actions

State cyber police units since 2024 have begun to cite both the Information Technology Act, 2000 and the Bharatiya Nyaya Sanhita, 2023 in the same FIR when they uncover mule account factories, crypto conversion centres, or phishing infrastructures that piggyback on legitimate corporate KYC pipelines; this was seen in large fraud busts in Alwar and Lucknow where officers booked the accused under IT Act provisions for unauthorised access and under "Section 318 of the Bharatiya Nyaya Sanhita, 2023" for cheating based on digital inducement, while also calling for records from the private bank whose employees allegedly enabled

[15] Rohas Nagpal, *Introduction to Indian Cyber Law* 75 (Asian School of Cyber Laws, Pune, 1st edn., 2008).
[16] 2022 CERT-In Directions on Reporting Cyber Incidents, *available at:* https://trilegal.com/wp-content/uploads/2022/05/2022-CERT-In-Directions-on-Reporting-Cyber-Incidents-1.pdf (last visited on November 1, 2025).

the scheme. In such investigations, officers look first at the organisation that failed to stop misuse of its platform, and where logs show that alerts were raised but no escalations followed, the material allows addition of "Section 85 of the Information Technology Act, 2000" against the company and its officers, especially if the compromised accounts were opened or continued in violation of internal SOPs. This pattern should be read with "Section 105 of the Bharatiya Nagarik Suraksha Sanhita, 2023" on audio-video recording of search and seizure, because it improves the evidentiary value of digital devices collected from corporate premises and makes later objections on chain of custody harder to sustain.[17]

1.4.3 DPDP Act Penalties

The DPDP Act's schedule empowers the Board to impose up to "₹250 crore for failure to take reasonable security safeguards to prevent personal data breach" and up to "₹200 crore for failure to notify" and current official commentary suggests that by virtue of the power in "Section 33(1) of the Digital Personal Data Protection Act, 2023" these ceilings can be revised, subject to an overall cap of double the amount already prescribed, which means Indian companies must now plan for a worst-case exposure that rivals or exceeds combined IT Act and sectoral penalties. The Board can start an inquiry on receipt of breach information from CERT-In, from a data principal, or from its own monitoring, and it may require production of policies, vendor contracts, DPIAs and breach logs, all of which will mirror what was or was not done under "Rule 3 and Rule 4 of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021", so any inconsistency can be read as neglect and ground a vicarious prosecution under "Section 85 of the Information Technology Act, 2000." Since the DPDP Act does not provide criminal punishment for corporate non-compliance but does not displace other laws, police are free to register BNS offences where data was misappropriated or used to aid organised crime, resulting in parallel tracks that push boards to frontload cyber investments.[18]

1.5 SPECIFIC CORPORATE RISK SCENARIOS

Corporate liability in cyber matters often crystallises around recurring fact clusters that show an avoidable gap between statutory expectations and what the board actually funded or monitored, and these clusters cut across sectors because attackers re-use access vectors while regulators and police re-use evidentiary theories. Indian threat reports for 2024-25 show rapid growth in financially motivated intrusions, double-extortion ransomware, insider-credential abuse, and misuse of digital platforms for investment fraud, and each such event links back to a duty under the IT Act, the DPDP Act or the 2021 IT Rules, creating space to attribute the event to failure of those who were in charge at the time. Where the corporation is an intermediary, the safe harbour in "Section 79 of the Information Technology Act, 2000" is available only if due diligence under

[17] Alwar Cops Bust 500-Cr Cyberfraud Network, Arrest 6 Accused, *available at:* https://timesofindia.indiatimes.com/city/jaipur/alwar-cops-bust-500-cr-cyberfraud-network-arrest-6-accused/articleshow/124200145.cms (last visited on October 29, 2025).

[18] Digital Personal Data Protection Act, 2023: DPDPA Section 7 With Interpretation, *available at:* https://dpdpa.com/theschedule.html (last visited on October 28, 2025).

the Rules is demonstrated, so failure to act on lawful orders or to keep traceable logs breaks the statutory shield and re-opens personal exposure, turning a simple cyber incident into a corporate criminal problem.[19]

1.5.1 Insider Data Exfiltration

Insider-driven theft of codebases, AI training data, financial models or customer datasets continues to be one of the hardest incidents to spot early because access often appears legitimate, yet once the download or transfer is detected the statutory picture becomes sharp. Unauthorised downloading, copying or extraction of data from a protected system attracts "Section 43 read with Section 66 of the Information Technology Act, 2000" and the corporation whose systems were misused can seek civil compensation for the loss; at the same time, if the exfiltrated content contains digital personal data, the company as data fiduciary must notify under the DPDP Act and demonstrate that role-based access controls, logging, and vendor NDAs were in place, failing which the Board can treat the event as absence of reasonable security safeguards. Police commonly pair such incidents with "Section 318 of the Bharatiya Nyaya Sanhita, 2023" for cheating or with "Section 316 of the Bharatiya Nyaya Sanhita, 2023" for criminal breach of trust where the employee stood in a position of trust, and the fact that the employer could not prevent the breach may be cited to inquire whether directors discharged duties under "Section 85 of the Information Technology Act, 2000."[20]

1.5.2 Ransomware and Breach Management

Ransomware incidents now attract more than technical remediation because CERT-In's 2024 ransomware notes advise reporting of even failed attempts, and the DPDP Act penalises any failure to notify breaches that compromise personal data, so a company that delays public disclosure in hope of decryption ends up breaching two central directions at once. Where forensic review shows that the intrusion succeeded due to lack of MFA, unpatched VPNs, unsegmented backups or absence of EDR despite prior alerts, prosecutors may argue that the company failed to put in place reasonable security practices as required under "Section 43A of the Information Technology Act, 2000" and under the DPDP schedule, opening the gate for vicarious liability of officers under "Section 85." If the ransomware group exfiltrated data and used it to commit cheating or identity theft against customers, police may, after July 2024, record offences under the corresponding BNS provisions and ask for corporate cooperation under the BNSS audio-video search provisions; non-cooperation or inconsistent statements then strengthen the case that officers were negligent. This makes breach management not only a technology response but a criminal risk containment exercise.[21]

1.5.3 Platform Abuse and UGC Harms

Platforms that host user-generated content or enable transactions sit in a fragile position because their business side often seeks to moderate, rank or monetise content, yet the more curatorial the activity, the easier it is for complainants and regulators to argue that the platform crossed from passive carriage into active

[19] India Cyber Threat Report 2025, *available at:* https://www.dsci.in/files/content/knowledge-centre/2024/India-Cyber-Threat-Report-2025.pdf (last visited on October 27, 2025).

[20] Section 318 BNS (Bharatiya Nyaya Sanhita): Cheating Provisions & Cases, *available at:* https://testbook.com/judiciary-notes/section-318-bns (last visited on October 26, 2025).

[21] Ransomware Attack: An Evolving Targeted Threat, *available at:* https://www.meity.gov.in/static/uploads/2024/03/Ransomware_Attack_An_Evolving_Targeted_Threat.pdf (last visited on October 25, 2025).

participation and so cannot claim automatic safe harbour. The decision in "*Shreya Singhal v. Union of India*[22], read "Section 79" to mean that intermediaries must act on court or government orders and not on every private complaint, but this benefit is contingent on full compliance with the 2021 IT Rules and the 2022-23 amendments that introduced the Grievance Appellate Committee and wider due diligence duties, which means that a platform that ignores or delays a valid takedown may lose statutory protection. Once safe harbour is lost, any BNS offence such as "Section 318" cheating through fake investment channels or organised cybercrime under "Section 111 of the Bharatiya Nyaya Sanhita, 2023" can be attributed to the platform's failure to act, and police can press for officer liability under "Section 85 of the Information Technology Act, 2000" on the ground that the default occurred with their consent or connivance.[23]

1.6 COMPLIANCE ARCHITECTURE AND GOVERNANCE

A sustainable corporate response to rising cyber prosecutions in India rests on creating governance structures that convert statutory timelines and evidentiary requirements into standing processes, so that when an incident occurs, the company can prove to CERT-In, the DPDP Board and criminal courts that lapses, if any, were not due to deliberate indifference by the management. This calls for boards to read cyber not as an IT budget issue but as a source of personal exposure because "Section 85 of the Information Technology Act, 2000" squarely penalises every person who was in charge of and responsible for the conduct of business when the contravention took place, unless that person proves due diligence. The BNSS 2023 also expects audio-video documentation of searches and better electronic record handling, which means companies must maintain accurate time-stamped logs, preserve emails that record board-level approvals, and maintain incident registers, all of which, when presented in courts under the BSA 2023, will help show reasonable care and may avert custodial interrogation of senior officers.[24]

1.6.1 Governance by Design

A governance-by-design approach for Indian corporates in 2025 would begin with the board formally designating a senior executive as accountable officer for IT Act, CERT-In, DPDP and IT Rules 2021 compliance and recording this in board minutes, because such an appointment can later support the statutory defence under "Section 85(1) proviso" that the contravention occurred without the knowledge of other directors. The board must receive periodic dashboards on incident reports filed with CERT-In, breach notices sent to the Data Protection Board, and SAR/LEA requests received from state cyber cells; such board oversight is important because any mismatch between actual incidents and what was reported to the board can be characterised as suppression. Internal audit cycles should be aligned to the CERT-In directions on log retention and time synchronisation, to BNSS search-and-seizure recording rules, and to the DPDP obligations on data processor contracts, so that audits cover both technical controls and legal documentation. Regular

[22] *(2015)5SCC 1*

[23] Shreya Singhal v. Union of India, *available at:* https://www.casemine.com/judgement/in/5790b244e561097e45a4e264 (last visited on October 24, 2025).

[24] Susan W. Brenner, *Cybercrime and the Law: Challenges, Issues, and Outcomes* 154 (Northeastern University Press, Boston, 1st edn., 2012).

interaction with sectoral regulators, including sharing of anonymised threat intelligence, also signals good faith, which becomes relevant when courts consider whether custodial interrogation of officers is needed.[25]

1.6.2 Incident Response Playbook

An Indian corporate incident response plan in the post-2022 environment must integrate time synchronisation, asset inventory, logging, evidence preservation, legal approval, and 6-hour disclosure into a single script that can be triggered any time of day, because CERT-In directions do not differentiate between weekdays and holidays and DPDP breach notification timelines also expect promptness. The plan should require SOC teams to capture volatile memory, system images, firewall and VPN logs, and to store them in India in a format that satisfies "Sections 61 to 63 of the Bharatiya Sakshya Adhiniyam, 2023", while the legal team prepares the first report to CERT-In and a parallel narrative for senior management. There must be a provision for cross-functional drills involving HR, procurement, PR, finance and infosec, as police and DPDP Board queries often arrive simultaneously and demand responses on employee conduct, vendor contracts and public communications. A preserved and signed chain-of-custody log, video recordings of seizure wherever BNSS requires, and an immediate hold on affected employee accounts help the company later show that it aided the investigation rather than obstructing it.[26]

1.6.3 Vendor and Intermediary Controls

Many corporate breaches originate in third-party managed services, AI annotation vendors, payment gateways or cloud-based content moderation partners, so contracts with such entities must reference Indian data localisation, log retention and notice requirements drawn from CERT-In and the DPDP Act, and must include rights to audit, insist on patched systems and insist on use of Indian time sources. Where the company acts as an intermediary or online marketplace, vendor onboarding should capture KYC, proof of lawful business and an undertaking to comply with all takedown orders, because loss of safe harbour due to third-party misconduct will otherwise rebound on the platform under "Section 79" read with the IT Rules 2021 and allow a prosecuting agency to invoke "Section 85" on the platform's directors. Vendor risk assessments should also map whether the partner is itself a data processor under the DPDP Act and whether it will notify the principal entity of sub-processor breaches in time for the latter to satisfy the Board; failure here can turn an external breach into an internal governance failure. Documented reviews every quarter and retention of correspondence enable the company to produce evidence before courts and regulators without delay.[27]

1.7 JUDICIAL RESPONSE: KEY DOCTRINAL MOVES

Indian courts over the last two decades have moved steadily to close historical excuses used by companies to avoid criminal accountability in technology-related cases, and these rulings now provide the doctrinal bedrock for prosecutors who want to combine IT Act contraventions, BNS offences and DPDP non-

[25] Gianclaudio La Diega, "The Internet of Citizens: A Lawyer's View on Some Technological Trends", 12 *Indian Journal of Law and Technology* 95 (2016).

[26] How to Comply With the CERT-In India 6 Hours Timeline?, *available at:* https://www.ardentprivacy.ai/blog/how-to-comply-with-the-cert-in-6-hours-timeline/ (last visited on October 23, 2025).

[27] Giancarlo Frosio, "Reforming Intermediary Liability in the Platform Economy", 13 *Indian Journal of Law and Technology* 112 (2017).

compliance in the same prosecution. The Supreme Court in the early 2000s was faced with arguments that a juristic person cannot be put in jail and so cannot be prosecuted for offences that prescribe mandatory imprisonment, yet the Court refused to accept this and held that the company could still be prosecuted and fined, while the natural persons could receive custodial sentences. Later, in a case concerning alleged misrepresentations in a securities offering, the Court said that a corporation can possess mens rea through those who control its affairs. Finally, in 2015, the Court read down intermediary liability to protect lawful speech while keeping the door open for liability when due process-based notices are ignored. This trilogy defines the current enforcement space.[28]

1.7.1 Prosecution of Corporates Despite Custodial Sentences

In "*Standard Chartered Bank v. Directorate of Enforcement*[29], the Supreme Court rejected the contention that a company could not be prosecuted for offences where the statute prescribed a sentence of imprisonment and fine together, pointing out that to accept such an argument would place corporations beyond the reach of many regulatory statutes. This holding is directly relevant to cybercrime-related corporate prosecutions because many IT Act offences and allied economic offences envisage imprisonment, and boards sometimes argue that since the company cannot be sent to jail, proceedings should stop. After Standard Chartered this line of defence lost force, so police and specialised agencies now file charge sheets naming the company and its responsible officers; the company is fined if found guilty, while officers face jail and fine. This ensures that when CERT-In or the DPDP Board forwards a case to law enforcement, the corporate entity cannot claim immunity merely due to its juristic character.

1.7.2 Attribution of Intent to Corporations

"*Iridium India Telecom Ltd v. Motorola Inc.*[30] settled the second plank by holding that corporations can be attributed the necessary mens rea in offences such as cheating, because the directing mind and will of the company are those who make decisions on its behalf. This is crucial for cybercrime settings where the offence is not the attack itself but the conscious decision not to patch a known vulnerability, not to encrypt sensitive personal data, or to keep running a fraudulent platform after law enforcement notices. Prosecutors can now draft charges stating that the company, acting through named officers, had knowledge of CERT-In orders, or of recurring phishing using the company's infra, yet failed to act, thereby satisfying the mental element of BNS offences like "Section 318" or of contraventions under the IT Act. The Iridium approach fits comfortably with "Section 85 of the Information Technology Act, 2000", which already envisages liability where the offence was committed with consent or connivance of any director, manager or secretary.[31]

[28] Farooq Ahmad, *Cyber Law in India (Law on Internet)* 178 (Pioneer Books, New Delhi, 1st edn., 2001).
[29] *(2005)4SCC 530.*
[30] *(2911)1SCC 74.*
[31] Iridium India Telecom Limited v. Motorola Incorporated & Others (2011) 1 SCC 74: Corporate Criminal Liability for Cheating, *available at:* https://lawfullegal.in/iridium-india-telecom-limited-v-motorola-incorporated-others-2011-1-scc-74-corporate-criminal-liability-for-cheating/ (last visited on November 1, 2025).

1.7.3 Calibrating Safe Harbour

"*Shreya Singhal v. Union of India*[32], recalibrated the scope of safe harbour by reading "Section 79" to mean that intermediaries are obligated to take down content only upon receiving actual knowledge in the form of a court order or a notice from a government agency, not upon every private complaint, and this clarification became the anchor for corporate defence in many cyber-defamation and UGC-related cases. Yet the same judgment also affirmed that due diligence rules framed by the Central Government remain binding, which became important after the 2021 IT Rules expanded such due diligence and created compliance positions like Chief Compliance Officer and nodal officer, non-compliance with which can lead to loss of safe harbour. For companies facing police action for phishing pages, loan app scams or deepfake pornography hosted on their platforms, Shreya Singhal offers a conditional shield, but once an authorised notice is ignored, prosecutors can fall back on "Section 85 IT Act, 2000" and on BNS provisions dealing with conspiracy or organised crime to reach the platform.

1.8 COMPARATIVE NOTES WITHIN INDIA

The transition from the Indian Penal Code, 1860 to the Bharatiya Nyaya Sanhita, 2023 and from advisory to mandatory CERT-In directions has changed the background assumptions for cybercrime investigations without altering the core principle that corporate actors can be made vicariously liable. BNS, effective from 1 July 2024, retains offences for cheating, criminal breach of trust, forgery, cyberstalking and sexual offences but renumbers them and, in some cases, increases punishment, which matters for BNSS provisions that now make forensic investigation compulsory where imprisonment is seven years or more. Simultaneously, CERT-In directions have made it much harder for corporations to argue that they had no knowledge of an incident or that logs were unavailable, since log retention in India and time-source synchronisation are now mandatory. This dual change means that where police earlier booked IPC cheating and relied on partial logs, they will now book "Section 318 BNS" and rely on preserved system logs backed by BSA-compliant certificates, leading to tighter prosecutions.[33]

1.8.1 IPC Regime to BNS 2023

Under the IPC regime, cyber-enabled cheating and breach of trust were usually booked under "Sections 420 and 406 IPC" with allied provisions on forgery, and courts often saw arguments about whether a civil breach had been dressed up as a criminal case. With BNS 2023, these offences are consolidated and renumbered as "Section 318" for cheating and "Section 316" for criminal breach of trust, with certain enhancements in punishment and clearer language on digital and electronic records as property, which allows police to frame charges that expressly speak of datasets, system credentials or tokens. Since the BNSS also enables electronic service of summons, audio-video recording of search and seizure, and wider powers to summon electronic communications, corporate custodians will be required to comply faster, making concealment harder. For

[32] *(2015)5 SCC1*

[33] New Sections in Criminal Laws: Cheating Is Not Section 420 but 318, Punishment for Murder Is Section 103, *available at:* https://indianexpress.com/article/explained/everyday-explainers/new-criminal-laws-cheating-sections-9426322/ (last visited on October 31, 2025).

corporate internal investigations, this means HR and legal teams must update their SOPs, disciplinary notices, and charge sheets to refer to the correct BNS provisions, failing which accused employees may claim procedural irregularity, and police may question the seriousness of the corporate response.[34]

1.8.2 Pre and Post CERT-In Directions

Before April 2022 many companies reported incidents at their convenience or only when sectoral regulators demanded it, so cyber police often worked with incomplete evidence, leading to closure reports or compounding. After the 2022 CERT-In directions, which continue to apply in 2025 and are now referenced by other regulators, every specified cyber incident must be reported within six hours and logs must be preserved in India for 180 days, which has radically improved the quality of digital evidence available to investigators. This means that in post-direction cases, when a company pleads that it did not know of the attack or that it could not preserve logs, investigators can point to a statutory obligation that was disobeyed and can recommend prosecution under "Section 85 of the Information Technology Act, 2000" for officers who were responsible at the time. The mandatory nature of these directions has also encouraged companies to create 24x7 SOCs and to sign up with managed detection providers, because delay is no longer defensible in front of the DPDP Board or criminal courts.[35]

1.9 CONCLUSION

Indian law is now close to a harmonised model where the Information Technology Act, 2000 supplies the vicarious liability engine through "Section 85", the DPDP Act, 2023 supplies high-value monetary disincentives through its schedule and Board-led inquiries, and the Bharatiya Nyaya Sanhita, 2023 supplies criminal labels that are future proof and digitally aware, while the BNSS and BSA, 2023 update procedure and evidence rules so that cyber incidents can be proved in court without technical dispute. For doctrinal coherence, future legal drafting, including the proposed Digital India Act, should expressly state that where a body corporate has (i) reported to CERT-In on time, (ii) cooperated with BNSS-compliant searches, and (iii) disclosed breaches to the DPDP Board and affected principals, prosecution of officers should be proportionate and focused on cases of consent, connivance or gross neglect. Courts following "*Standard Chartered Bank v. Directorate of Enforcement*[36], *Iridium India Telecom Ltd v. Motorola Inc.*[37] and "*Shreya Singhal v. Union of India*[38] can continue to affirm corporate accountability while still protecting intermediaries that act promptly on lawful notices and maintain the audit trails now demanded by CERT-In. The research path ahead lies in testing how DPDP penalties interact with criminal confiscation under other

[34] Corresponding Section Table of Bharatiya Nyaya Sanhita, 2023 (BNS) With Indian Penal Code, 1860 (IPC), *available at:* https://uppolice.gov.in/site/writereaddata/siteContent/Three New Major Acts/20240628171056482 3BNS_IPC_Comparative.pdf (last visited on October 30, 2025).

[35] Michael Karanicolas, "Authoritarianism as a Service: India's Moves to Weaponize Private-Sector Content Moderation with the 2021 IT Rules", 17 *Indian Journal of Law and Technology* 214 (2021).

[36] *(2005)4 SCC 530.*

[37] *(2011) 1 SCC 74.*

[38] *(2015)5 SCC 1*

economic laws and how far draft Digital India Act proposals will recalibrate safe harbour for curated platforms.

1.10 SUGGESTIONS:

Building on the analysis of corporate liability in cybercrimes and the evolving judicial response, the following ten recommendations translate doctrine into boardroom action.

1. Establish a single "digital incidents and evidence" charter at board level. Mandate a named accountable officer for IT-Act/CERT-In/DPDP/IT-Rules compliance in board minutes and publish an internal order mapping deputies and after-hours escalation. Require quarterly certifications from CISO, DPO and platform-compliance leads that Section 85 due-diligence artefacts (policies, logs, takedown registers) are current. Tie senior-management variable pay to audit-verified compliance outcomes.
2. Operationalise the six-hour CERT-In window with a 24×7 "one-button" playbook. Pre-approve templates for initial and follow-up notifications, with time-synced screenshots and volatile-memory captures auto-attached. Instrument all critical systems to Indian NTP sources and auto-hash log bundles to an in-India evidence vault. Include a legal sign-off checkpoint that cannot block transmission beyond T+4 hours.
3. Rebuild intermediary due diligence around measurable SLAs. For valid court/government orders, hard-wire takedown within the mandated hours; for sexual imagery or impersonation, enforce 24-hour removal with case IDs and preserved artefacts. Publish monthly transparency metrics (acknowledgement in 24 hours; disposal in 15 days; LEA response within 72 hours). Run spot tests where the legal team issues dummy notices to verify end-to-end compliance.
4. Institutionalise documentation for the Section 85 defences. For every material incident, assemble a "reasonableness file" within 72 hours: policy excerpts, control screenshots, training rosters, prior audit findings, and board-level reviews. Require each responsible officer to append a dated narrative of actions taken, with timestamps aligned to Indian NTP sources. Store these files immutably; they are your first line of defence if vicarious liability is later alleged.

BIBLIOGRAPHY

Books:

- Anirudh Rastogi, Cyber Law: Law of Information Technology and Internet (LexisNexis, New Delhi, 1st edn., 2014).
- Farooq Ahmad, Cyber Law in India (Law on Internet) (Pioneer Books, New Delhi, 1st edn., 2001).
- Nappinai N. S., Technology Laws Decoded (LexisNexis, New Delhi, 1st edn., 2017).
- Pavan Duggal, Cyber Law (Universal Law Publishing, New Delhi, 1st edn., 2016).
- Rahul Matthan, Privacy 3.0: Unlocking Our Data-Driven Future (HarperCollins, Gurugram, 1st edn., 2020).
- Rohas Nagpal, Introduction to Indian Cyber Law (Asian School of Cyber Laws, Pune, 1st edn., 2008).
- Susan W. Brenner, Cybercrime and the Law: Challenges, Issues, and Outcomes (Northeastern University Press, Boston, 1st edn., 2012).
- Talat Fatima, Cyber Crimes (Eastern Book Company, Lucknow, 1st edn., 2011).

Statutes:

- The Bharatiya Nagarik Suraksha Sanhita, 2023 (Act No. 46 of 2023)
- The Bharatiya Nyaya Sanhita, 2023 (Act No. 45 of 2023)
- The Bharatiya Sakshya Adhiniyam, 2023 (Act No. 47 of 2023)
- The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023)
- The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (G.S.R. 139(E), dated 25-02-2021; as amended on 06-04-2023)
- The Information Technology Act, 2000 (Act No. 21 of 2000)

Articles:

- Chinmayi Arun, "Gatekeeper Liability and Article 19(1)(a) of the Constitution", 7 NUJS Law Review 15 (2014).
- Giancarlo Frosio, "Reforming Intermediary Liability in the Platform Economy", 13 Indian Journal of Law and Technology 85 (2017).
- Gianclaudio La Diega, "The Internet of Citizens: A Lawyer's View on Some Technological Trends", 12 Indian Journal of Law and Technology 95 (2016).
- Michael Karanicolas, "Authoritarianism as a Service: India's Moves to Weaponize Private-Sector Content Moderation with the 2021 IT Rules", 17 Indian Journal of Law and Technology 200 (2021).
- Nivedita Saksena, "An Analysis of the Modern Offence of Sedition", 7 NUJS Law Review 121 (2014).
- Sejal Chandak, "Continuing Discrimination in the Times of Technology: Women, Work, Algorithms and Law in India", 19 Indian Journal of Law and Technology 30 (2023).

- Umakanth Varottil, Mihir Naniwadekar, "Vicarious Liability of Directors: New Directions?", 23 National Law School of India Review 109 (2011).
- Vasudev Devadasan, "Conceptualising India's Safe Harbour in the Era of Platform Governance", 19 Indian Journal of Law and Technology 10 (2023).

Websites:

- 2022 CERT-In Directions on Reporting Cyber Incidents, available at: https://trilegal.com/wp-content/uploads/2022/05/2022-CERT-In-Directions-on-Reporting-Cyber-Incidents-1.pdf (last visited on November 1, 2025).
- Alwar Cops Bust 500-Cr Cyberfraud Network, Arrest 6 Accused, available at: https://timesofindia.indiatimes.com/city/jaipur/alwar-cops-bust-500-cr-cyberfraud-network-arrest-6-accused/articleshow/124200145.cms (last visited on October 29, 2025).
- Corporate Criminal Liability and Securities Offerings: Rationalizing the Iridium-Motorola Case, available at: https://docs.manupatra.in/newsline/articles/Upload/C12A50C0-74C8-4819-8F6A-9CB4D286CCB1.pdf (last visited on October 23, 2025).
- Correspondence Table and Comparison Summary of the Bharatiya Nyaya Sanhita, 2023 (BNS) to the Indian Penal Code, 1860 (IPC), available at: https://bprd.nic.in/uploads/pdf/COMPARISON SUMMARY BNS to IPC .pdf (last visited on October 25, 2025).
- Corresponding Section Table of Bharatiya Nyaya Sanhita, 2023 (BNS) With Indian Penal Code, 1860 (IPC), available at: https://uppolice.gov.in/site/writereaddata/siteContent/Three New Major Acts/20240628171056482 3BNS_IPC_Comparative.pdf (last visited on October 30, 2025).
- Decoding the Proposed IT Amendment Rules, 2025, available at: https://theleaflet.in/digital-rights/law-and-technology/decoding-the-proposed-it-amendment-rules-2025 (last visited on October 31, 2025).
- Digital Personal Data Protection Act, 2023: DPDPA Section 7 With Interpretation, available at: https://dpdpa.com/theschedule.html (last visited on October 28, 2025).
- Directions Under Sub-Section (6) of Section 70B of the Information Technology Act, 2000 Relating to Information Security Practices, Procedure, Prevention, Response and Reporting of Cyber Incidents for Safe & Trusted Internet, available at: https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf (last visited on October 31, 2025).
- How to Comply With the CERT-In India 6 Hours Timeline?, available at: https://www.ardentprivacy.ai/blog/how-to-comply-with-the-cert-in-6-hours-timeline/ (last visited on October 23, 2025).
- India Cyber Threat Report 2025, available at: https://www.dsci.in/files/content/knowledge-centre/2024/India-Cyber-Threat-Report-2025.pdf (last visited on October 27, 2025).
- Iridium India Telecom Limited v. Motorola Incorporated & Others (2011) 1 SCC 74: Corporate Criminal Liability for Cheating, available at: https://lawfullegal.in/iridium-india-telecom-limited-v-motorola-incorporated-others-2011-1-scc-74-corporate-criminal-liability-for-cheating/ (last visited on November 1, 2025).

- New Criminal Laws to Be Effective From 1st July 2024, available at: https://www.cyberpeace.org/resources/blogs/new-criminal-laws-to-be-effective-from-1st-july-2024 (last visited on October 30, 2025).
- New Sections in Criminal Laws: Cheating Is Not Section 420 but 318, Punishment for Murder Is Section 103, available at: https://indianexpress.com/article/explained/everyday-explainers/new-criminal-laws-cheating-sections-9426322/ (last visited on October 31, 2025).
- Ransomware Attack: An Evolving Targeted Threat, available at: https://www.meity.gov.in/static/uploads/2024/03/Ransomware_Attack_An_Evolving_Targeted_Threat.pdf (last visited on October 25, 2025).
- Section 318 BNS (Bharatiya Nyaya Sanhita): Cheating Provisions & Cases, available at: https://testbook.com/judiciary-notes/section-318-bns (last visited on October 26, 2025).
- Section 85 - The Information Technology Act, available at: https://lawgist.in/information-technology-act/85 (last visited on October 26, 2025).
- Shreya Singhal v. Union of India, available at: https://www.casemine.com/judgement/in/5790b244e561097e45a4e264 (last visited on October 24, 2025).
- Shreya Singhal vs U.O.I on 24 March, 2015, available at: https://indiankanoon.org/doc/110813550/ (last visited on November 1, 2025).
- Standard Chartered Bank and Ors v. Directorate of Enforcement, available at: https://journal.lawmantra.co.in/?p=142 (last visited on October 24, 2025).
- The Bharatiya Nagarik Suraksha Sanhita, 2023, available at: https://prsindia.org/billtrack/the-bharatiya-nagarik-suraksha-sanhita-2023 (last visited on October 28, 2025).
- The Digital Personal Data Protection Act, 2023, available at: https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf (last visited on November 1, 2025).
- The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 [Updated as on 6.4.2023], available at: https://www.meity.gov.in/static/uploads/2024/02/Information-Technology-Intermediary-Guidelines-and-Digital-Media-Ethics-Code-Rules-2021-updated-06.04.2023-.pdf (last visited on October 29, 2025).
- The Information Technology Act, 2000, available at: https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf (last visited on October 27, 2025).