CYBER CRIME UNDER THE INFORMATION TECHNOLOGY ACT: NATIONAL PERSPECTIVE

Tusshar Sharma, Guru Gobind Singh Indraprastha University

1. Introduction

The advent of the cyberspace as the inseparable part of the modern human life has radically changed the nature and the field of the criminal activity in the XXI century. Due to the fact that India is moving towards a digital economy where more than 86 per cent of households are now connected to the internet and more than 820 million users are now operating within the digital realm, India is at the same time being exposed to vulnerabilities and threats in ways that never existed within a traditional geographical space and a traditional jurisdictional boundary. In its modern form, cybercrime is a somewhat complex phenomenon where computers, networks, and digital infrastructure can both be used as tools to perpetrate crimes or become the target of malicious activities and is thus a complex web of legal, technological, and social problems that requires advanced regulation solutions.

The process of developing a well-developed legal framework applicable in the context of cybercrime in India began with the adoption of the Information Technology Act, 2000, which put the country in the twelfth position among the countries worldwide in adopting special legal framework in dealing with cybercriminals. This was an innovative law which came as a reply to the United Nations Commission on International Trade Law (UNCITRAL) Model law on electronic commerce which was an indication of India acknowledging the need to give a legal standing to electronic transactions and at the same time lay down a deterrent to undesirable digital practices. The next amendment in 2008 saw a paradigm shift in the cyber legal regime in India as strict provisions were adopted to deal with the new menaces such as cyber terrorism, child sexual abuse content, identity theft and intrusion into systems without permission- some of which the initial Act of 2000 had failed to tackle.

The current situation in cybersecurity in India offers a paradox: on the one hand, technological development and digitalization have enabled new opportunities and levels of economic growth and social inclusion by implementing the Digital India program, on the other hand, they have

created a new favorable environment in which advanced criminal networks can operate and exist across the borders and take the advantage of technological flaws. The increase of cybercrime of 10.29 lakh to

22.68 lakh incidents between 2022 and 2024 is not only a 206 percent change in financial losses of Rs. 22,845 crore, but also a complete change in the criminal tactics, sophistication of the perpetrator, and susceptibility of the victim. CRM Financial frauds based on the manipulation of unified payment interface (UPI), phishing attacks, ransomware-as-a-service activities, money laundering with the help of cryptocurrencies, deepfakes fraud, and AI-assisted sextortion have become the key threat vectors against the Indian digital environment.

The Information ATechnology act, 2000, even in its pioneering position and subsequent amendments, is gradually proving to contain structural constraints in harnessing the emerging threat environment. The structure of the Act, based on the technological realities of the early 2000s when the internet has only penetrated 0.5% of the population, needs extensive updating to meet the new technology of artificial intelligence, quantum computing, blockchain, internet of things (IoT), and 5G networks. This paper looks at cybercrime according to the Indian legal system with special reference to the national viewpoint, the statutory provisions and the framework of punishments, the institutional provisions to enforce and coordinate the cybercrime, investigations, and the various complex issues that face the Indian cyber legal system. Integrating legal texts and empirical evidence about the current threat environment and the ways institutions respond, this discussion will offer a broad overview of the regulation of cybercrime in India and pinpoint areas in which the cyber legal system has failed to match the rapidly growing digitalized society and offer evidence-based suggestions on how this system can be improved to safeguard people, companies, and infrastructure.

2. The Law in India: The Constitution and Legislation of Cyber Crime.

2.1 The Information Technology Act, 2000, has undergone evolution.

The Information Technology Act, 2000 is the most important law enforcement tool in India to govern the cyberspace and deal with the growing threat of computer crimes in the new age of digital technology. This ground breaking law was passed on the 17th of October 2000 as a response to the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce to accord legal status to electronic transactions and digital

signatures and to offer a broad framework to address cyber crimes. The Act is an Indian effort to establish a secure and trustful digital environment that strikes the right balance between technological progress and legal protections, which will lead to e-commerce, e-governance, and electronic communication in the wide digital environment of India.

The initial Act was greatly transformed under the Information Technology (Amendment) Act, 2008 whereby it brought massive changes in the Act given that there were new cyber threats which the earlier legislation had not sufficiently addressed. This amendment signified a paradigm change in the attitude of India regarding the subject of cybersecurity by adding the provisions of increased privacy of data, information security, and corporate responsibility towards the protection of the digital environment. One of the amendments that came in 2008 was the introduction of critical sections that dealt with modern cybercrimes such as Section 66A (asset struck down) on offensive messages, increased penalties to various cyber offenses, child pornography under Section 67B, cyber terrorism under Section 66F and broadening the definition of intermediary liability under Section 79. Moreover, the amendment accepted the authority of Indian Computer Emergency Response Team (CERT-In) and redefended digital signature technology to be technology neutral and thus made the legislation to be flexible to the changing technology standards.

2.2 The basics of Rights and Cyber Jurisprudence.

Indeed, constitutional aspects of cyber law in India have been significantly influenced by the historic judicial decisions that have determined the balancing act among individual liberties and state control over cyberspace. The Supreme Court ruling in Shreya Singhal v Union of India (2015). was the watershed moment in the history of Indian cyber jurisprudence. Where the highest court quashed under Article 19(1) (a) of the constitution guaranteeing freedom of speech and expression millions of Indian citizens were subjected to the law of Section 66A of the Information Technology Act, 2000 as declared illegal in the case of , it held that Section 66A of the Information Technology Act, 2000 was unconstitutional. The Court declared that the Section 66A was too diffuse that it could be arbitrarily applied, and was not able to pass the test of reasonable restrictions of Article 19(2) of the Constitution. This clause had criminalized the transmission of messages that are offensive by way of communication services but the Court concluded that it did not include the nexus required between the forbidden speech and actual harm and that it constituted a chilling effect on lawful speech in

the Internet world.

The logic of the Shreya Singhal case determined by the Supreme Court provided important precedents in terms of assessing cyber laws in the context of constitutionality. The Court pointed out that the state has valid concerns in regulating digital communication, but it should be specific, strictly focused, and limited not too far to prevent the violation of the main freedoms in an arbitrary and haphazard way. The ruling also made it clear that Section 66A did not draw the distinction between mass communication that could incite a disturbance in the population and private communication that could simply irritate a person thus reaching very far beyond the limits that the Constitution allows. Justice K.S. Puttaswamy v Union of India (2017). was another pioneer to cyber jurisprudence. , where the Supreme Court pronounced that the right to privacy was a fundamental right in the Constitution of Article 21. This case resulted in significant ramifications to data protection legislations and cybersecurity procedures, including the constitutional principles of all subsequent digital rights and the decision-making process of the Digital Personal Data Protection Act, 2023. All these judicial interventions have influenced the cyber legal landscape in India positively by confirming that digital expression is entitled to the same constitutional protection as other forms of expression as well as acknowledging the role of the state in ensuring that citizens are free of real cyber threats.

3. Classification and Dimensions of Cyber Offences

3.1 Statutory Provisions and Penalty Structure

The amended Information Technology Act, 2000, offers an elaborate categorization of cyber offenses along with the penalties attached to them, which are divided in several parts. Section 43 of the Act imposes civil liability in a case of unauthorized access to computer system, introduction, downloading, copying, or extracting data without authorization, interference of system functioning, or denying an authorized individual access, and compensates damages of this kind of unauthorized activities up to 1 crore. In case of actions as described in the Section 43 committed with ill-intends of dishonesty or fraudulent nature, they become criminal offences under the Section 66 and this makes the person face imprisonment up to three years or a fine up to 5 lakh or both. The Act additionally outlines certain cyber crimes by use of specific sections: Section 65 defines tampering with computer source documents as a criminal offense, which carries a sentence up to three years imprisonment or a fine of no more than 2

lakh or both; Section 66B criminizes receipt of stolen computer resources or communication devices with unfaithfulness, and it is punishable with up to three years in jail or a fine of not more than 1 lakh or both.

Section 66C is particularly concerned with identity theft and associated crimes and punishes the dishonest use of electronic signatures, passwords, or unique features of identification of another individual providing imprisonment up to three years or a fine up to 1 lakh of money or both. Section 66D is specifically aimed at cheating by personation with the help of a computer resource, and punishment is the same as in 66D, but in Section 66E, it concerns a violation of privacy by means of unauthorized capturing, publishing, or transmitting of personal pictures, which is punishable by imprisonment up to 3 years or a fine of RS. 2 Lakh or both. The worst of them is Section 66F, which tackles cyber terrorism whose possible punishment is life imprisonment in the event that the act is done with an intention of disturbing the unity, integrity, security or sovereignty of India or causing terror to the people. The crimes of publishing or transmission of obscene and sexually explicit material are contained in Section 67 (publishing or transmitting obscene material in electronic form), Section 67A (publishing or transmitting a material containing sexually explicit acts), and most importantly in Section 67B touching on child pornography, where the punishment is imprisonment of seven years plus a fine amounting to Rs. 10 lakh. Also, Section 70 makes it a crime to gain access or even seek to gain access to secured systems, and the punishment includes imprisonment of ten years and fine, whereas breach of confidentiality and privacy is addressed by Section 72 which implies a fine of Rs. 5 lakh.

3.2 Modern Cyber Threat Environment.

The situation with the cyber threats in India has been characterized by a chilling effect of the number and the sophistication of the attacks as the country experience an increasing digital footprint and cybersecurity infrastructure weaknesses. The Ministry of Home Affairs presented data to the Parliament revealing that the Indians had lost an incredible 22,845.73 crores to cyber fraud in 2024, which drastically increased by 206 percent of the reported 7,465.18 crores in 2023. This was an exponentially increasing financial losses which were subsidized by 36.37 lakh cases of financial fraud recorded through the National Cyber Crime Reporting Portal (NCRP) and Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS) in 2024 as compared to 24.42 lakh cases recorded last year. The annual

distribution can be summarized as the following: 10.29 lakh cases of reported cybercrime occurred in 2022 (a growth of 127.44% per year), 15.96 lakh cases were reported in 2023 (an increase of 55.15% year-on-year), and 22.68 lakh cases occurred in 2024 (an increase of 42.08 per year).

Cybercrimes have significantly changed, and those are of various attack vectors with a wide range of traditional-hacking and identity theft to more advanced phishing schemes, ransomware attacks, online financial frauds, and more so, AI-driven deep fake frauds. The use of financial frauds via manipulation of unified payment interface (UPI), QR code scam, SIM swap fraud, and email spoofing have become the most common forms of threats that attack the rapidly growing digital payment system in India. Materials of child sexual abuse (CSAM), online sextortion, cyberstalking and cyber harassment are serious issues that have impacted vulnerable groups especially women and children. The statistics reveal that the majority of cybercrimes now moved to the cryptocurrency platforms exploiting the anonymity and decentralization of the blockchain technology to avoid the conventional law enforcement system (over 90 percent). Even a more worrying outlook by experts estimates that cybersecurity attacks in India have the potential to increase to the claim of one trillion attacks per annum in the 2033-2047 spectrum, compared to 79 million attacks per annum, a growth pace that is exponentially rising. The fact that India has been ranked as the third-largest digital economy in the world with an internet user base of over 820 million and transactions of over 10 billion monthly via UPI, makes it a potential victim of cybercriminals, and requires innovative, dynamic and tech-savvy countermeasures.

4. Mechanisms and Architecture of Enforcement.

4.1 National Infrastructure and Indian Cyber Crime Coordination Centre.

The Indian Cyber Crime Coordination Centre (I4C), which will be located within the Ministry of Home Affairs and created in 2020, is the heart of the Indian system in the institutional support of the fight against cybercrime in a coordinated and holistic way. I4C, a nodal point to counter cybercrime at the national level and develop an effective coordination of law enforcement agencies across states and union territories, was inaugurated in Home Minister Amit Shah in New Delhi in January 2020 after approval in October 2018 at a budget of Rs. 415.86 crore. The Centre has seven interlinked elements which are meant to establish a comprehensive ecosystem on cybercrime prevention, detection, investigation and prosecution.

These elements consist of the National Cyber Crime Threat Analytics Unit (TAU) which examines and reports threats, the National Cyber Crime Reporting Portal (NCRP) through which citizens can register complaints round the clock, the National Cyber Crime Training Centre (NCTC) where the capacity of law enforcement staff is developed, the Cyber Crime Ecosystem Management Unit where awareness is created, the Platform of Joint Cyber Crime Investigation Team where inter-state coordination in cyber crime is facilitated, the National Cyber Crime Research and Innovation Centre where indigenous forensic tools are developed and the I4C has also initiated a number of ground breaking initiatives in order to enhance the capability of India in combating cybercrime. In August 2019, the National Cyber Crime Reporting Portal (www.cybercrime.gov.in) was operationalized that gives citizens a platform to report any form of cyber crime, although crimes against women and children receive particular attention. The portal has received large number of complaints since its inception, as 317,439 cyber crime cases and 5,771 FIRs have been registered by February 2021, which shows the effectiveness of using this portal as a centralized reporting channel. The reporting and management system of financial frauds called Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS) is accompanied by a national toll-free helpline number, 1930 that allows immediate reporting of financial frauds so that the authorities can freeze or recover the siphoned funds on a near-real-time basis. This has been an enormously effective system that has saved more than Rs. 5,489 crore in 17.82 lakh complaints lodged in 2024. There was also the Suspect Registry, took over by I4C along with banks and other financial institutions in September 2024, where over 11 lakh identifiers of suspects were gathered and over 24 lakh mule accounts were flagged, which prevented an estimated Rs. 4,631 crore in fraud. I4C has added the Pratibimb module, which visualizes cybercriminal networks and infrastructure on a geographic scale and allows enforcers to take action encouraged across jurisdictions and has resulted in 10,599 arrests, 26,096 linkages identified, and 63,019 investigative assistance requests.

4.2 | Investigation Procedures and Adjudication Framework

In India, under the new Bharatiya Nagarik Suraksha Sanhita (BNSS), there is an upgrading in the procedures of cybercrime investigation, as compared to the previous regime. BNSS, 2023 also enables police officers, even those who do not hold an inspected position, to investigate cognizable cyber offences, along with the encouragement of expeditious registration of FIR and electronic filing; in case an informant has presented a complaint electronically, it has to

be signed within three days in order to have formal FIR registered.

One of the major reforms relates to the fact that the recording of all search and seizure procedures is compulsory and is audio-video recorded, provided by Section 105 BNSS which guarantees the transparency and integrity of collecting digital evidence. These procedures should be recorded by the police which should be forwarded immediately to the magistrate. BNSS also demands the mandatory forensic investigation of cyber-offences, which have sentences seven years or longer, which promotes the requirements of evidence preservation and gathering. The BNSS and the Bharatiya Sakshya Adhiniyam 2023 strengthen the admissibility of electronic evidence, provides the protocols in the storage and transfer of electronic evidence, and permits the trial proceedings to be conducted through electronic means.

Clarity in jurisdiction is enhanced: the BNSS enables investigation of crimes when one of the data or suspects is in India, which is consistent with the new procedural protections and minimises potential ambiguity on extra-territorial jurisdiction. Judgement and appeals have become more transparent and technology-enabled hearings, and the focus on forensic chain of custody and audit trails at every level has been renewed, which has enhanced justice of cybercrime in India by making it quicker and more reliable.

5. Difficulties, Future Projections and Policy Requirements.

5.1 Jurisdictional Bottlenecks and Implementation Dilemmas.

The cyberspace is transnational and borderless and this poses a great challenge in jurisdiction which has greatly impeded effective implementation of cyber laws in India. Many cybercrimes are trans-national where the perpetrators are based in one country, the servers in another, the victims in a third country, and the money laundering finances in another country and the legal and practical barriers to investigating and prosecuting these crimes are complex. Where crimes target computer resources in India, section 75 of the Information Technology Act renders extra-territorial jurisdiction in an effort to extraterritorially apply the Act. But the application of such provisions is faced with great challenges such as the absence of mutual legal assistance treaties (MLATs) with a considerable number of countries and delays in receiving evidence in foreign jurisdictions, differences in the definition of cybercrime across legal system, and the lack of harmonised international legal frameworks.

The jurisdictional theories that are applicable to cybercrimes are subjective territoriality (when the act is committed on the territory of the forum state), objective territoriality/ effects jurisdiction (when the main impact of the act is experienced in the territory of the forum state even though it is performed elsewhere), and passive personality jurisdiction (when the action is directed to a victim of nationality). A fact that can be seen is the pragmatism that has been assumed by the Indian courts in deriving the jurisdiction which was seen in cases that applied Section 179 of the Code of Criminal Procedure which provides the jurisdiction upon the basis of which anything was done or consequence had occurred in relation to the crime. But the problems of enforcement do not only end with the jurisdictional issue but also include the lack of technical infrastructure to deal with cybercrime, the lack of trained cyber forensic specialists and investigators, a lack of technical capacity within the law enforcement agencies, the difficulty in preserving volatile digital evidence, encryption and anonymization technology that prevents investigations, and coordination issues between central and state agencies. Withdrawal of general consent by eight states on CBI investigations by the parliamentary standing committee has given rise to operational delay in dealing with inter-state cybercrimes, and the recommendation to amend the Delhi Special Police Establishment Act, 1946, to enable CBI to investigate cybercrimes countrywide without state consent.

5.2 New Technologies and Policy reactions.

The convergence of the new technology and the cybercrime is not only offering new threats but also offers creative opportunities to enhance the cyber defense power of India. Artificial intelligence and machine learning have become two-sided swords in the cybersecurity arsenal: AIbased solutions allow to perform advanced threat identification, behavioral analytics, and computer-assisted incident response, but at the same time, they can grant cybercriminals the ability to perform advanced phishing attacks, deepfakes to commit fraud and manipulate others, polymorphic malware to avoid the conventional detection systems, and zero-day vulnerabilities at an increased rate. The 442% growth rate of voice-based phishing attacks based on AI-generated content proves that cyber threats are becoming increasingly sophisticated. Security Information and Event Management (SIEM) systems powered by AI can be considered a radical solution to cyber defense, with machine learning being deployed to handle large amounts of security event data in real time to facilitate perceiving threats and automatic responses, reducing the response time by orders of magnitude in comparison to a more traditional signature-driven approach to detection.

The policy response of India to changing cyber threat involves various aspects such as legislation changes, capacity building of institutions, technological development and international collaboration. The Data Security Council of India (DSCI) has produced the National Cyber Security Strategy which outlines 21 major focus areas that will help in development of secure, reliable, resilient cyberspace promoting growth and trust (created in 2020 under the leadership of Lt. General Rajesh Pant (National Cybersecurity Coordinator). The plan focuses on enhancing cyber defense against critical information infrastructure, improving internet infrastructure in the light of the economic situation in India in the context of ICT and IT-enabled services, developing technical standards and promoting Brandon India in cybersecurity, improving cyber diplomacy and international cooperation, enhancing cyber insurance platforms, and enhancing cybercrime investigations through innovation and strategic investment. The amendment of the Allocation of Business Rules in September 2024 facilitated the administration of cybersecurity in India through delegating cybersecurity issues to the Ministry of Electronics and Information Technology (MeitY), cyber crime to the Ministry of Home Affairs, telecom network security to the

Department of Telecommunications and overall coordination and the strategic direction to the National Security Council Secretariat (NSCS) to create a hub-and-spoke model with a centralized coordination and varying roles.

6. Conclusion

Prevention and creating awareness is an important aspect of the holistic strategy of dealing with cybercrime in India. The government has also initiated massive awareness efforts using the portals such as www.infosecawareness.in and www.csk.gov.in to supply educational information that is directly designed to children, parents and general users on information security best practices. The Cyber Crime Volunteers Program of I4C consists of citizens who are interested in serving the country to become part of the cybercrime prevention model, establishing a participatory system of cyber defense. The Centre has also required cyber forensic-cum-training laboratories in 28 states as part of the Cyber Crime Prevention against Women and Children (CCPWC) scheme which offers financial aid in setting up cyber forensic laboratories, training of the law enforcement personnel, prosecutors and judicial officers, and employing junior cyber consultants to bridge the expertise gaps. It has also been implemented concretely through law enforcement by blocking more than 9.42 lakh SIM cards and 2.63 lakh

IMEI numbers associated with cyber fraud which has proven to have operational efficacy in dismantling cybercriminal networks.

The future outlook of cybercrime in India will be determined by some of the most important aspects such as the implementation of zero-trust architecture principles that involve constant verification of users and devices, the possible effect of quantum computing on encryption standards and vulnerability discovery, the dual potential of blockchain technology to facilitate crimes based on cryptocurrencies and provide a higher level of security in digital transactions, the vulnerability of the Internet of Things (IoT) to security threats as billions of networked devices increase the attack space, the security issues of 5G networks due to high-connectivity speeds and the spread of devices The creation of special programs called Cyber Commandos in states and union territories is meant to have special wings of trained workers that are capable of addressing the changes in cyber security threats. Researchers have forecasted that detecting the combination of agentic AI will raise the effectiveness of defenders by an order of magnitude, and at the same time, the market price of exploits will decrease to trifles due to the increased ability of AI to find zero-day exploits. As India works towards its vision of achieving a 5 trillion economy, enhancing cybersecurity infrastructure, aligning laws and technologies, developing niche human capital, developing and sustaining the public-private partnerships and keeping pace with emerging threats will have been the crucial step to achieving a safe, trusted, and resilient digital ecosystem that empowers citizens without compromising national interests.

BIBLIOGRAPHY

PRIMARY SOURCES – STATUTORY PROVISIONS

1. The Information Technology Act, 2000, Ministry of Communications and Information Technology, Government of India. (Principal legislation governing cybercrime in India)

2. The Information Technology (Amendment) Act, 2008, Official Gazette of India. (Paradigm shift introducing Sections 66F (cyber terrorism), 67B (child pornography), and enhanced penalties)

3. The Bharatiya Nyaya Sanhita, 2023, Ministry of Law and Justice, Government of India. (New criminal code replacing Indian Penal Code, 1860, effective July 1, 2023)

4. The Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS), Ministry of Law and Justice, Government of India. (New criminal procedure code replacing Code of Criminal Procedure, 1973, with enhanced provisions for cybercrime investigation)

5. The Bharatiya Sakshya Adhiniyam, 2023 (BSA), Ministry of Law and Justice, Government of India. (New evidence law replacing Indian Evidence Act, 1872, with modernized digital evidence provisions)

6. The Indian Evidence Act, 1872, Ministry of Law and Justice, Government of India. (Section 65B on electronic records; partially superseded by BSA, 2023)

7. The Code of Criminal Procedure, 1973, Ministry of Law and Justice, Government of India. (Section 165 on collection of digital evidence; partially superseded by BNSS, 2023)

8. The Protection of Children from Sexual Offences Act, 2012 (POCSO Act), Ministry of Women and Child Development. (Section 15 on child sexual abuse material; interpreted with Section 67B of IT Act)

9. Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013, Ministry of Communications and Information Technology. (Governs CERT-In operations and cyber incident reporting)

10. Information Technology (Procedure and Safeguards for Blocking of Access of

Information by Public) Rules, 2009, Ministry of Communications and Information Technology. (Governs blocking of content under Section 69A of IT Act)

LANDMARK CASE LAW – SUPREME COURT

11. Shreya Singhal v. Union of India, (2015) 5 SCC 1, Supreme Court of India (W.P. (Crim.) No. 167 of 2012). (Struck down Section 66A of IT Act as unconstitutional; watershed moment protecting free speech in digital sphere)

12. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, Supreme Court of India (Writ Petition No. 494 of 2012). (Nine-judge bench verdict establishing right to privacy as fundamental right under Article 21; critical for cyber law and data protection)

13. Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473, Supreme Court of India. (Landmark ruling on admissibility of electronic evidence and Section 65B of Indian Evidence Act)

14. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 2 SCC 361, Supreme Court of India. (Clarified authentication requirements for electronic evidence; influenced BSA, 2023 provisions)

15. State of Tamil Nadu v. Suhas Katti, Supreme Court of India. (First conviction under Section 67 of IT Act for publishing obscene material; established procedural framework for cybercrime trials)

16. Internet and Mobile Association of India v. Reserve Bank of India, (2020) 3 SCC 1, Supreme Court of India. (Lifted RBI ban on cryptocurrency trading; relevant to cybercrime involving digital assets and ransomware payments)

17. XYZ v. Union of India, Supreme Court of India, 2024 (Reiterated companies must implement robust data security measures; strengthened cyber liability regime)

18. Om Prakash Ambadkar v. State of Maharashtra, 2025 SCC OnLine SC 238, Supreme Court of India. (Clarified magistrate's role under Section 175(3) of BNSS in ordering cybercrime investigations)

19. Union of India v. Builders Association, Supreme Court of India, 2025. (Case regarding jurisdiction and investigation powers under BNSS for cyber-related financial frauds)

20. Harish (POCSO Case), Supreme Court of India, September 2024. (Overturned Madras High Court ruling; held that viewing, storing, and possessing child pornography is punishable under POCSO Act and Section 67B of IT Act)

HIGH COURT PRECEDENTS

21. Madras High Court v. Harish, 2024 (Initially ruled viewing of child pornography not criminal; overturned by Supreme Court; important for Section 67B interpretation

22. Delhi High Court v. Nasscom v. Ajay Sood & Others, March 2005, Delhi High Court.

    (Declared phishing illegal; first judicial recognition of phishing as passing off and tarnishing identity)

23. Orissa High Court – Section 175(3) BNSS Petition, 2025 SCC OnLine Orissa HC. (Reiterated magistrate must hear police before ordering cybercrime investigation under BNSS)

24. Karnataka High Court Judgment on Cryptocurrency Fraud, 2023-2024 series. (Addressed cyber fraud involving cryptocurrency platforms; interpreted DVT and jurisdictional provisions)

25. Bombay High Court Cyber Terrorism Case, Post-2008 Amendment. (First case applying Section 66F (cyber terrorism) provisions after IT Amendment Act, 2008)

26. Gujarat High Court on Digital Evidence Chain of Custody, 2024. (Established standards for maintaining chain of custody of digital evidence under BNSS and BSA

27. Tamil Nadu Cyber Crime Special Court v. Various Accused, Suhas Katti case precedent series. (Series of early cybercrime convictions establishing evidentiary standards)

CASE LAW – LOWER COURTS AND CRIMINAL COURTS

28. Arif Azim Case, CBI Cybercrime Matter. (First cybercrime conviction in India under Sections 418, 419, 420 IPC; precedent for hybrid cybercrime-traditional crime charges)

29. Jogesh Kwatra Case, Civil Suit for Defamation via Email. (Early case on sending derogatory emails; established civil liability under Section 43 of IT Act)

30. Thomas Cook Limited Case, Cybercrime Cell Investigation (First case on identity fraud and cyber attacks in hospitality sector; enhanced security standards post-investigation)

31. Elgar Parishad/Bhima Koregaon Case (BK-16), Pune Police Investigation, 2014-2024. (Significant case involving malware (NetWire RAT) attacks; highlighted digital evidence manipulation and forensic challenges)

32. Ravin Khosla v. Unknown, Delhi Cyber Crime Cell. (Case on online harassment and cyberstalking; tested provisions of Sections 354A and 354D of IPC read with IT Act sections)

LAW JOURNAL ARTICLES AND PUBLICATIONS

33. Bandu B. Meshram & Dr. Manish Kumar Singh, "From FIR to Forensic Analysis in the Digital Age: Legal Powers, Investigative Models, and Judicial Oversight of Cybercrime Policing in India," International Journal for Research and Development, 2025. (Comprehensive analysis of BNSS 2023, BSA 2023, and IT Act integration; forensic protocols)

34. Shashank Mohan Gupta & Dr. Astitwa Bhargava, "Digital Evidence in Indian Criminal Law: Admissibility and Authenticity under the BSA, 2023," Indian Journal of Legal and Legal Research, October 2025. (Paradigm shift in electronic evidence treatment; Section 63(4) BSA analysis)

35. Sameer Patil, "Adequacies and Inadequacies in Cyber Forensics: Technical Infrastructure and Conviction Rates in India," Observer Research Foundation (ORF) Policy Brief, December 2022. (Analysis of low conviction rates, forensic challenges, and resource constraints in cyber investigation)

36. Kartikey Srivastava, "Section 66A, Information Technology Act, 2000, Shreya Singhal Case: An Alternative Perspective," LiveLaw Legal Analysis, November 2021. (Pre- and post-Shreya Singhal jurisprudence on offensive speech; misuse patterns)

37. Dr. Rajesh Pant (National Cybersecurity Coordinator), "National Cyber Security Strategy 2020," Ministry of Home Affairs & Data Security Council of India, 2020. (Policy framework with 21 focus areas; foundational document for cyber investigation infrastructure)

38. Judicial Academy, Jharkhand, "Cyber Crime Cases: Issues, Challenges & Solutions," Training Manual, February 2025. (Practical guide on investigation procedures, evidence collection, emerging threats including AI-driven attacks)

39. Dr. Shweta Tiwari, "Cryptography, Encryption, and Zero-Day Exploits: Barriers to Cybercrime Investigation in India," Journal of Criminal Law Research, 2023. (Technical barriers to cybercrime investigation; encryption and anonymization challenges)

40. Supreme Court Observer, "X Relies on 'Shreya Singhal' in Arbitrary Content-Blocking Case in Karnataka High Court," July 2025. (Analysis of Section 69A blocking orders vs. Section 79 intermediary safe harbor; procedural safeguards)

GOVERNMENT PUBLICATIONS AND INSTITUTIONAL REPORTS

41. Ministry of Home Affairs Parliamentary Data, "Cybercrime Statistics 2022-2024," Lok Sabha Statement, December 2022. (Official statistics: 10.29 lakh cases (2022), 15.96 lakh (2023), 22.68 lakh (2024); financial losses: INR 22,845.73 crore (2024))

42. Indian Cyber Crime Coordination Centre (I4C), "National Cyber Crime Reporting Portal (www.cybercrime.gov.in) Annual Report," Ministry of Home Affairs, 2024. (Statistics on complaints registered, FIRs filed; efficacy of centralized reporting mechanism)

43. Indian Cyber Crime Coordination Centre (I4C), "Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS) Report," 2024. (Data on INR 5,489 crore saved through 17.82 lakh complaints; Suspect Registry: 11 lakh suspects, 24 lakh mule accounts flagged, INR 4,631 crore prevented)

44. Indian Computer Emergency Response Team (CERT-In), "Direction on Information Security Practices, Procedures, Prevention, Response and Reporting of Cyber Incidents," April 28, 2022. (Mandatory reporting within 6 hours; Section 70B(6) of IT Act)

45. National Crime Records Bureau (NCRB), "Crime in India Reports 2022-2024," Ministry of Home Affairs. (Statistical analysis of cybercrime categories: financial fraud, child sexual abuse, identity theft, ransomware; conviction rates data)

46. Bureau of Police Research and Development (BPRD), "Use of Technology and Audio-Video Recording of Search and Seizure," Standard Operating Procedures, January 2025. (Implementation guidelines for Section 105 BNSS mandatory recording requirements)

47. Bureau of Police Research and Development (BPRD), "SOP of Audio-Video Recording for Scene of Crime," Technical Manual, 2024. (Procedural safeguards for digital evidence preservation; chain of custody protocols)

48. CONTEMPORARY LAW REVIEW ARTICLES – STATUTORY REFORMS

49. JSA Law Advisors, "Stringent Measures Against Cybercrimes in India's New Criminal Justice System (BNSS, BSA, BNS)," Newsletter, JSA Law, 2024-2025. (Analysis of enhanced powers under BNSS for cyber investigation; comparison with CrPC regime)

50. Nishitha Desai Associates, "Cyber Crime Under Bharatiya Nyaya Sanhita: Challenges and Opportunities," Legal Publication, March 2025. (Analysis of BNS 2023 cyber offense provisions; sentencing frameworks; emerging threat responses)

51. Argus Partners, "CERT-In's Six-Hour Reporting Rule for Cyber Security Incidents: Statutory Provisions and Global Comparisons," Thought Paper, 2024. (Comparative analysis of India's CERT-In reporting mandate vs. global standards; compliance penalties under Section 70B(7) of IT Act)