AN ANALYSIS OF THE EXISTING LEGAL FRAMEWORK FOR NEW AGE CYBERCRIMES IN INDIA

Dr. Chanjana Elsa Philip, Associate Professor, CMR University School of Legal Studies, Bengaluru

Rahul Gadhoke, LL.M. (Criminal Law), CMR University School of Legal Studies, Bengaluru

ABSTRACT

India's digital revolution has rapidly reshaped the nation over the past decade, but this progress comes with growing cybersecurity concerns. As technology evolves, so do the methods of cybercriminals, posing serious threats to national security, personal privacy, and public trust. The country's current legal framework often falls short in effectively addressing these modern cyber offenses. The ***Information Technology Act, 2000*** remains the cornerstone of cyber law in India, yet it requires significant updates to tackle the complexities of today's digital threats. Traditional provisions under the ***Indian Penal Code, 1860*** are similarly inadequate when applied to cyber-specific crimes. This research explores the pressing need to strengthen India's legal response to cybercrime. It critically examines whether the existing laws and enforcement mechanisms can keep pace with the evolving nature of digital offenses. The study highlights gaps in legislation, enforcement challenges, and the need for more empowered cyber-specific courts and investigative bodies. It also draws on international best practices, offering valuable lessons for India's fight against cyber threats. Emerging dangers like deepfake misuse, cryptocurrency fraud, AI-driven cyberattacks, and social media manipulation require urgent legal attention. The growing frequency of data breaches also threatens democratic institutions and individual rights. Through a doctrinal research approach, this study analyses statutory laws, key judgments, and relevant policy documents. Comparative insights from other jurisdictions further enrich the findings. Ultimately, this research emphasizes the urgent need for holistic legal reforms to build a robust, future-ready cybersecurity framework in India.

Keywords: Cybercrime, Information Technology Act, Digital Security, Cyber Forensics, Data Protection, Constitutional Rights, International Cooperation, Legal Framework.

INTRODUCTION

A. Background and Context of Cybercrime in India

India emerged as a global technology hub following economic liberalization in 1991. The telecommunications revolution transformed communication patterns across urban and rural areas. Internet penetration surged from 0.5% in 2000 to over 50% by 2023. This digital transformation created unprecedented opportunities for economic growth and social development.[1]

However, rapid digitization also spawned new categories of criminal activities. Cybercriminals exploited technological vulnerabilities to commit sophisticated offenses across digital platforms. Traditional crimes migrated online while entirely new forms of digital misconduct emerged. The National Crime Records Bureau documented substantial increases in cybercrimes over the past decade.[2] Financial frauds, identity theft and data breaches became commonplace across India's digital landscape.

Government initiatives like Digital India accelerated the country's technological adoption significantly. The program aimed to transform India into a digitally empowered society. E-governance platforms, digital payment systems and online service delivery became integral to public administration. Over 138 crore Aadhaar cards were issued creating the world's largest biometric database.[3] This massive digitization of personal information attracted cybercriminals seeking to exploit stored data.

The COVID-19 pandemic further accelerated digital transformation across all sectors. Remote working arrangements increased dependency on digital infrastructure and cloud services exponentially. Educational institutions shifted to online learning platforms creating new vulnerabilities. Healthcare systems adopted telemedicine and digital health records extensively.

[1] Telecom Regulatory Authority of India, 'Performance Indicators Reports' (TRAI) http://www.trai.gov.in/release-publication/reports/performance-indicators-reports accessed 30 May 2025

[2] National Crime Records Bureau, 'Crime in India 2018 - Volume 1' (Ministry of Home Affairs 2019) https://www.thehinducentre.com/resources/article30555357.ece/binary/Crime%20in%20India%202018%20-%20Volume%201.pdf accessed 30 May 2025

[3] Unique Identification Authority of India, 'Annual Report 2022-23' (UIDAI 2023) https://uidai.gov.in/images/UIDAI_Annual_Report-2022-23_English.pdf accessed 30 May 2025

This rapid shift exposed organizations to sophisticated cyber threats including ransomware attacks.[4]

Financial digitization through Unified Payments Interface revolutionized India's payment ecosystem. UPI transactions reached record levels processing over 74 billion transactions valued at ₹139 trillion annually. Digital wallets, online banking and cryptocurrency trading gained widespread acceptance among users. Yet this growth attracted cybercriminals who exploited payment system vulnerabilities through phishing attacks.[5] Banking frauds involving digital channels caused substantial financial losses to institutions and consumers.

This research adopts a comprehensive doctrinal methodology approach. The study relies primarily on analysis of existing legal texts and judicial pronouncements. Statutory provisions under The Information Technology Act, 2000 form the core analytical framework. The research examines relevant sections of the "Bhartiya Nyaya Sanhita", concerning digital offenses. Case law analysis includes landmark judgments from the Supreme Court and High Courts. Secondary sources include academic commentaries, government reports, and policy documents from the Ministry of Electronics and Information Technology.

UNDERSTANDING NEW AGE CYBERCRIMES: CONCEPTUAL FRAMEWORK

A. Definition and Classification of Cybercrimes

Cybercrime encompasses criminal activities conducted through digital platforms and computer networks systematically. The term gained prominence with internet technology advancement in the late twentieth century. Legal scholars define cybercrime as offenses committed using computers as instruments or targets. The "Bharatiya Nyaya Sanhita", 2023 now provides the primary legislative framework for cybercrime in India.[6]

The Supreme Court in *State of Tamil Nadu v. Suhas Katti* recognized cybercrime as a distinct category of criminal offense. This landmark case established the first conviction under the IT Act in 2004. The Court emphasized that cybercrimes transcend geographical boundaries unlike

[4] Ministry of Electronics and Information Technology, 'Cyber Security Reports' (Government of India 2023)
[5] National Payments Corporation of India, 'UPI Product Statistics' (NPCI) https://www.npci.org.in/what-we-do/upi/product-statistics accessed 30 May 2025
[6] "Bharatiya Nyaya Sanhita" 2023, s 111

traditional crimes. Digital evidence and virtual crime scenes characterize these offenses fundamentally.[7]

Classification systems for cybercrimes vary across jurisdictions and academic literature significantly. The United Nations Office on Drugs and Crime categorizes cybercrimes into core and enabled offenses. Core cybercrimes target computer systems directly while enabled crimes use technology as tools. This classification helps law enforcement agencies develop targeted investigation strategies.[8] The "Bharatiya Nyaya Sanhita" recognizes cybercrime as part of organized crime under Section 111. This provision defines organized crime to include cybercrimes committed by crime syndicates. The BNS treats cybercrime with enhanced penalties when committed as organized criminal activity. Financial scams and cyber-related offenses carry severe punishments under this framework.[9]

B. Emerging Threats in the Digital Era

Artificial intelligence-powered cyber attacks represent the latest evolution in cybercriminal methodologies substantially. Machine learning algorithms enable automated vulnerability discovery and exploitation techniques effectively. Cybercriminals deploy AI to create sophisticated phishing campaigns with personalized content strategically. Voice phishing attacks increased by 442% in 2024 due to AI-generated impersonation tactics.[10] Deepfake technology poses unprecedented challenges to legal systems and evidence authentication mechanisms. Criminals create synthetic media content to manipulate public opinion and commit fraud. The technology enables identity impersonation for financial crimes and reputation damage. Section 353 of the BNS addresses misinformation including through electronic means.[11]

---

[7] State of Tamil Nadu v Suhas Katti, CC No 4680 of 2004, Additional Chief Metropolitan Magistrate, Egmore (5 November 2004) https://lawbhoomi.com/state-of-tamil-nadu-vs-suhas-katti/ accessed 30 May 2025

[8] United Nations Office on Drugs and Crime, 'Comprehensive Study on Cybercrime' (UNODC 2013) https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf accessed 30 May 2025

[9] 'Overview of the "Bharatiya Nyaya Sanhita", 2023' (AZB Partners, 8 January 2024) https://www.azbpartners.com/bank/overview-of-the-bharatiya-nyaya-sanhita-2023-penal-code/ accessed 30 May 2025

[10] 'Deepfake Defense in the Age of AI' (The Hacker News) https://thehackernews.com/2025/05/deepfake-defense-in-age-of-ai.html accessed 30 May 2025

[11] 'Countering Misinformation; Provisions under the "Bharatiya Nyaya Sanhita", 2023' (CyberPeace Foundation, 9 September 2024) https://www.cyberpeace.org/resources/blogs/countering-misinformation-provisions-under-the-bharatiya-nyaya-sanhita-2023 accessed 30 May 2025

Cryptocurrency-related crimes have proliferated with the growth of digital asset markets exponentially. Criminals exploit the pseudonymous nature of blockchain transactions for money laundering activities. Ransomware operators demand payments in cryptocurrencies to avoid traditional banking monitoring systems. The BNS treats financial frauds involving digital assets as serious organized crime. Internet of Things devices create expansive attack surfaces for cybercriminals to exploit effectively. Smart home devices, industrial control systems and medical equipment lack adequate security measures. Criminals compromise IoT networks to launch distributed denial-of-service attacks systematically. "The SonicWall Cyber Threat Report noted 107% surge in IoT malware attacks during 2024."[12]

OVERVIEW OF INDIA'S CYBERCRIME LEGAL ARCHITECTURE

A. Constitutional Framework and Fundamental Rights in Cyberspace

The constitutional framework governing India's cyberspace emanates from "Part III of the Constitution which enshrines fundamental rights." H.M. Seervai observes in his seminal work Constitutional Law of India that fundamental rights serve as "constitutional restraints over the state's authority to intervene within the protective gamut of civil liberties." These constitutional protections extend to digital environments creating a legal foundation for cybercrime regulation.[13]

"Article 19(1)(a) guarantees freedom of speech and expression which the Supreme Court has extended to digital communications." M.P. Jain notes in Indian Constitutional Law that "the freedom of speech and expression includes the right to express one's thoughts through any medium including electronic means." This constitutional principle creates both opportunities and challenges for cybercrime regulation as online speech requires balanced protection.[14] The constitutional position regarding privacy in cyberspace was definitively established in "*K.S. Puttaswamy v. Union of India"*. The nine-judge bench declared privacy as a fundamental right under Article 21 stating that "privacy is an essential aspect of human dignity and forms the

[12] 'Top 10 Biggest Cyber Attacks of 2024 & 25 Other Attacks to Know About' (CM Alliance) https://www.cm-alliance.com/cybersecurity-blog/top-10-biggest-cyber-attacks-of-2024-25-other-attacks-to-know-about accessed 30 May 2025

[13] H.M. Seervai, Constitutional Law of India: A Critical Commentary (4th edn, Universal Law Publishing 2015) vol 1, 349

[14] "M.P. Jain, Indian Constitutional Law (9th edn, LexisNexis 2024) 1440"

core of the rights guaranteed by Articles 14, 19 and 21." This landmark judgment provides constitutional foundation for data protection and cyber privacy laws.[15]

Article 21's guarantee of life and personal liberty has been expansively interpreted to include digital rights. Seervai emphasizes that personal liberty encompasses "all varieties of rights" not specifically enumerated elsewhere. The Supreme Court's progressive interpretation includes digital privacy, informational autonomy and protection from cyber harassment within Article 21's ambit.[16] The constitutional framework requires cybercrime laws to satisfy the test of reasonableness under Article 19(2). Jain explains that reasonable restrictions must be "proportionate to the legitimate aim sought to be achieved." This constitutional requirement ensures that cybercrime legislation does not unduly infringe upon fundamental rights while addressing legitimate security concerns.[17]

The doctrine of technological neutrality ensures constitutional principles apply equally to physical and digital spaces. The Supreme Court in "*Anuradha Bhasin v. Union of India"* held that fundamental rights cannot be suspended merely because they are exercised through digital mediums. This principle mandates that cybercrime laws respect constitutional boundaries regardless of the technological context.[18] Article 14's equality guarantee extends to digital governance requiring non-discriminatory access to cyber justice mechanisms. Constitutional courts have recognized that equal protection includes equal access to digital infrastructure and cyber security protections ensuring that cybercrime laws do not create digital divides.[19]

B. The Information Technology Act, 2000: Genesis and Evolution

"The Information Technology Act, 2000" represents India's pioneering effort to establish comprehensive cybercrime legislation. Pavan Duggal, in his authoritative treatise Cyber Law, describes the Act as "India's first legislation dealing with cybercrimes and electronic commerce." The Act was enacted on October 17, 2000, responding to urgent need for legal framework governing digital transactions and cyber offenses.[20]

[15] K.S. Puttaswamy v Union of India (2017) 10 SCC 1
[16] H.M. Seervai, Constitutional Law of India: A Critical Commentary (n 1) vol 2, 1635
[17] M.P. Jain, Indian Constitutional Law (n 2) 1298
[18] Anuradha Bhasin v Union of India (2020) 3 SCC 637
[19] M.P. Jain, Indian Constitutional Law (n 2) 1156
[20] Pavan Duggal, Cyber Law: An Exhaustive Section-wise Commentary on the Information Technology Act (3rd edn, LexisNexis 2023) 25

The Act's genesis lies in the UNCITRAL Model Law on Electronic Commerce, 1996, which provided international framework for electronic transactions. Duggal notes that "the IT Act was drafted keeping in mind the UNCITRAL Model Law to ensure India's alignment with global standards." This international foundation enabled India to participate effectively in cross-border cyber legal cooperation.[21]

The original Act contained 94 sections organized into 13 chapters addressing electronic governance, digital signatures and cybercrime prevention. Karnika Seth observes in her cyber law writings that "the Act provided legal recognition to electronic records and digital signatures enabling e-commerce growth in India." The legislation established technological equivalence between digital and paper-based transactions.[22] The Act's enforcement mechanisms included establishment of Cyber Appellate Tribunal providing specialized adjudication. Duggal emphasizes that "the creation of specialized cyber courts marked India's recognition of the need for technical expertise in cyber jurisprudence." This institutional innovation addressed the complexity of technology-related legal disputes.[23]

The 2008 amendment significantly expanded the Act's scope introducing new cybercrime provisions. Seth notes that "the amendment addressed emerging threats like cyber terrorism, identity theft and child pornography." Section 66A criminalized sending "offensive messages" while Section 69 granted authorities interception powers reflecting evolving security challenges.[24] However, the constitutional validity of certain provisions faced judicial scrutiny. "The Supreme Court in *Shreya Singhal v. Union of India* struck down Section 66A holding it violated Article 19(1)(a). Justice Nariman observed that the provision was "arbitrarily wide and vague" lacking definitional clarity required for criminal legislation."[25]

The Act underwent further evolution through subordinate legislation including the IT Rules 2011 and subsequent amendments. Duggal notes that "these rules provided detailed implementation framework addressing intermediary liability and data protection." The regulatory framework continued adapting to technological developments and emerging cyber

[21] Pavan Duggal, Cyberlaw: The Indian Perspective (Saakshar Law Publications 2020) 45
[22] Karnika Seth, 'Cyber Law Book Excerpt' (2010) https://www.karnikaseth.com/cyber-law-book-excerpt-5.html accessed 30 May 2025
[23] Pavan Duggal, Cyber Law: An Exhaustive Section-wise Commentary on the Information Technology Act (n 8) 156
[24] Karnika Seth, 'Cybercrime Investigations and IT Act 2000' (ICAI Presentation 2013)
[25] Shreya Singhal v Union of India (2015) 5 SCC 1

threats.[26] Contemporary proposals for Digital India Act suggest comprehensive legislative overhaul. The proposed legislation would address artificial intelligence, algorithmic accountability and platform regulation. This evolution reflects the dynamic nature of cyberspace requiring continuous legal adaptation to technological advancement.[27]

C. The Information Technology (Amendment) Act, 2008: Key Modifications

The Information Technology (Amendment) Act, 2008 marked a pivotal transformation in India's cybercrime legal framework. This comprehensive amendment significantly expanded the scope and effectiveness of cyber law enforcement mechanisms. The original Information Technology Act, 2000 primarily focused on electronic commerce and digital signatures but lacked robust provisions for addressing emerging cyber threats.[28]

The 2008 amendment introduced revolutionary changes to combat sophisticated cybercriminal activities effectively. Parliament passed the amendment without any debate on 22nd December 2008 in the Lok Sabha. The Rajya Sabha subsequently approved it on 23rd December 2008 with similar swiftness. President Pratibha Patil granted assent on 5th February 2009, bringing the amendment into force. This rapid legislative process reflected the urgent need to address growing cybersecurity challenges facing the nation.

Section 66A emerged as one of the most controversial provisions introduced through this amendment. "This section penalized sending offensive messages through communication devices or computer resources. The provision criminalized transmission of information that was grossly offensive, menacing, or false. It also targeted messages sent with intent to cause annoyance, inconvenience, danger, obstruction or criminal intimidation."[29] The punishment prescribed included imprisonment up to three years along with monetary fines for violations.

However, Section 66A faced severe constitutional challenges due to its vague terminology and

[26] Pavan Duggal, Cyber Law: An Exhaustive Section-wise Commentary on the Information Technology Act (n 8) 234

[27] Pavan Duggal, 'Digital India Act: Future of Cyber Regulation' in Emerging Technologies and Law (CyberLaw Publications 2024) 78

[28] Pranesh Prakash, 'Short note on IT Amendment Act, 2008' (Centre for Internet and Society, February 2009) https://cis-india.org/internet-governance/publications/it-act/short-note-on-amendment-act-2008 accessed 30 May 2025

[29] "What is the Information Technology Amendment Act 2008 (IT Act 2008)?" TechTarget https://www.techtarget.com/whatis/definition/Information-Technology-Amendment-Act-2008-IT-Act-2008 accessed 30 May 2025

excessive scope. Legal experts criticized the provision for its arbitrary application and potential misuse against legitimate expression. The Supreme Court in Shreya Singhal v. Union of India ultimately struck down Section 66A as unconstitutional in 2015.[30] "The Court held that the provision violated Article 19(1)(a) of the Constitution guaranteeing freedom of speech and expression."

Section 69 introduced unprecedented government powers for interception, monitoring and decryption of electronic information. "This provision authorized Central and State governments to intercept any information transmitted through computer resources. The powers could be exercised in interests of sovereignty, integrity, defense, security or public order."[31] These surveillance capabilities provided law enforcement agencies with sophisticated tools for cybercrime investigation and prevention.

The amendment substantially expanded cybercrime definitions through Sections 66B to 66F addressing various digital offenses. "Section 66B criminalized dishonestly receiving stolen computer resources or communication devices. Section 66C introduced identity theft as a distinct cybercrime with specific penalties. Section 66D addressed punishment for cheating by personation using computer resources fraudulently."[32] These provisions filled critical gaps in the original legislation's coverage of emerging cyber threats.

Section 66E introduced significant privacy protections by criminalizing violation of personal privacy through electronic means. This provision specifically addressed voyeurism and unauthorized publication of private images without consent. The section recognized growing concerns about digital privacy violations in an increasingly connected society. Penalties included imprisonment up to three years and substantial monetary fines for violators.[33]

Section 66F established cyber terrorism as a distinct and serious criminal offense under Indian law. This provision addressed acts committed with intent to threaten unity, integrity, security or economic security of India. Cyber terrorism offenses also included acts intended to strike

[30] Shreya Singhal v Union of India (2015) 5 SCC 1
[31] 'Section 69A & Section 66(A) of the Information Technology (IT) Act' PMF IAS (14 December 2024) https://www.pmfias.com/section-69a-section-66a-of-the-it-act/ accessed 30 May 2025
[32] 'IT-Related Changes in the "Bharatiya Nyaya Sanhita" (BNS)' Law for Citizens https://lawforcitizens.com/it-related-changes-in-the-bharatiya-nyaya-sanhita-bns/ accessed 30 May 2025
[33] "Information Technology (Amendment) Act, 2008 Internet Democracy" https://internetdemocracy.in/laws/the-information-technology-amendment-act-2008/ accessed 30 May 2025

terror among people or disrupt essential services. The punishment prescribed included life imprisonment, reflecting the gravity of such offenses against national security.[34]

The amendment introduced revolutionary changes in digital evidence admissibility and authentication procedures significantly. Section 79A mandated appointment of Examiner of Electronic Evidence by the Central Government. These examiners provided expert opinions on electronic evidence in judicial proceedings and other legal forums. The provision enhanced the credibility and reliability of digital evidence in criminal prosecutions.[35]

D. Integration with Bharatiya Nyaya Sanhita

The Bharatiya Nyaya Sanhita, 2023 represents a paradigmatic shift in India's criminal law framework with significant implications for cybercrime prosecution. This legislation replaced the colonial-era Indian Penal Code while incorporating contemporary legal principles for digital age crimes. The integration between BNS and existing cyber laws creates a comprehensive framework for addressing modern criminal activities.[36]

Section 2(39) of BNS explicitly establishes harmonious integration with information technology legislation through definitional alignment. This provision ensures that technological terms maintain consistent meanings across both BNS and Information Technology Act. The integration prevents interpretational conflicts and jurisdictional confusion in cybercrime prosecutions. Legal practitioners benefit from unified terminology across different statutes addressing digital offenses.[37]

The BNS introduces Section 111 targeting organized crime with specific inclusion of cyber-crimes within its ambit. This provision addresses continuing unlawful activities committed by crime syndicates including digital offenses. However, the absence of clear cyber-crime

[34] P Madhava Soma Sundaram, "Information Technology Act and Cyber Terrorism: A Critical Review ResearchGate (August 2011)" https://www.researchgate.net/publication/228192670_Information_Technology_Act_and_Cyber_Terrorism_A_Critical_Review

[35] 'All about digital evidence' iPleaders (23 February 2024) https://blog.ipleaders.in/all-about-digital-evidence/ accessed 30 May 2025

[36] "The Bharatiya Nyaya Sanhita, 2023 PRS India" https://prsindia.org/billtrack/the-bharatiya-nyaya-sanhita-2023 accessed 30 May 2025

[37] "Changes Brought Forth by the Bharatiya Nyaya Sanhita, 2023 Lexology (4 July 2024)" https://www.lexology.com/library/detail.aspx?g=8b6e523a-8ba1-4575-9408-c58a70cd31cc accessed 30 May 2025

definitions creates interpretational challenges for enforcement agencies. The broad formulation allows flexibility but may lead to inconsistent application across different jurisdictions.[38]

Section 152 of BNS replaces the controversial sedition provision while addressing digital communication channels explicitly. "This section criminalizes acts endangering sovereignty, unity and integrity of India through electronic means. The provision covers encouragement of secession, armed rebellion and subversive activities transmitted through digital platforms. The reformulated approach attempts to balance national security concerns with constitutional free speech protections."[39]

Section 197(d) introduces specific provisions targeting false or misleading information disseminated through electronic channels significantly. This section addresses misinformation campaigns that jeopardize national integrity, security or public order. The provision recognizes the amplified impact of digital misinformation in contemporary society. However, critics argue that broad terms like "misleading information" could enable excessive censorship of legitimate discourse.[40]

Traditional criminal offenses under BNS receive enhanced applicability to digital contexts through interpretative expansion. Sections addressing theft, fraud, defamation and harassment encompass electronic manifestations of these crimes. Section 303 and 317 cover theft of mobile phones, data and computer hardware with appropriate penalties. Section 318 and 336 address various forms of fraud including cyber frauds and identity theft.[41]

The BNS strengthens provisions against crimes targeting women through digital platforms and electronic harassment. Section 74 addresses assault or criminal force against women with intent to outrage modesty including digital contexts. Section 75 specifically criminalizes sexual harassment through electronic means with enhanced penalties. These provisions recognize the

[38] 'The New Criminal Laws and Their Interface with Technology' Esya Centre (31 July 2024) https://www.esyacentre.org/perspectives/2024/7/31/the-new-criminal-laws-and-their-interface-with-technology
[39] "Cyber crime punishments under BNS (Bharatiya Nyaya Sanhita) MyJudix (19 February 2024)" https://www.myjudix.com/post/cybercrime-punishments-under-bns-bharatiya-nyaya-sanhita
[40] "Countering Misinformation; Provisions under the Bharatiya Nyaya Sanhita, 2023 CyberPeace Foundation (9 September 2024)" https://www.cyberpeace.org/resources/blogs/countering-misinformation-provisions-under-the-bharatiya-nyaya-sanhita-2023
[41] 'How is Cyberbullying tackled under the Law in India?' Rau's IAS (accessed 30 May 2025) https://compass.rauias.com/current-affairs/cyberbullying-tackled-law-india/

gendered nature of many cybercrimes and provide appropriate legal remedies.[42]

Defamation provisions under Section 356 of BNS explicitly cover electronic transmission of defamatory content. This section penalizes defamatory material sent through emails, social media and other digital platforms. The provision maintains traditional defamation principles while adapting to modern communication methods. Penalties include imprisonment and monetary fines reflecting the serious nature of reputational harm.

Section 351 addressing criminal intimidation extends seamlessly to digital threats and online harassment campaigns. This provision covers intimidation through electronic messages, social media posts and other digital communications. The broad formulation ensures comprehensive coverage of evolving intimidation tactics in cyberspace. Law enforcement agencies can prosecute various forms of online threats under this provision.

The BNS introduces petty organized crime provisions under Section 112 with specific relevance to minor cyber offenses. This category includes activities like selling examination papers online and small-scale digital frauds. The provision distinguishes between individual criminal acts and those committed by organized groups or gangs. Enhanced penalties apply when similar offenses are committed collectively rather than individually.[43]

E. Relevant Provisions under the The Bharatiya Nagarik Suraksha Sanhita 2023

The Bharatiya Nagarik Suraksha Sanhita 2023 represents a paradigmatic shift in India's criminal procedure framework. This legislation replaced the outdated Code of Criminal Procedure 1973 effective July 1, 2024. The BNSS specifically addresses contemporary challenges posed by cybercrime through technology-integrated provisions. These provisions demonstrate the legislature's commitment to modernizing investigative and judicial processes for the digital age.[44]

Section 105 of BNSS mandates audio-video recording of all search and seizure operations. This provision requires police officers to record search activities through electronic means including mobile devices. The recorded material must be forwarded immediately to designated

[42] ibid
[43] 'The Bharatiya Nyaya (Second) Sanhita, 2023' PRS India https://prsindia.org/billtrack/the-bharatiya-nyaya-second-sanhita-2023 accessed 30 May 2025
[44] Bharatiya Nagarik Suraksha Sanhita 2023, Preamble

magistrates along with seizure lists. This technological integration ensures transparency and accountability in evidence collection procedures. The provision significantly enhances the credibility of digital evidence in cybercrime investigations where procedural integrity remains paramount.[45]

The most significant procedural innovation appears in Section 176(3) which mandates forensic investigation for serious offenses. This provision requires forensic experts to visit crime scenes for offenses punishable by seven years or more imprisonment. The forensic collection process must be videographed on mobile phones or electronic devices by investigating officers. This mandatory videography creates an unalterable record of evidence collection procedures. The provision addresses critical gaps in cybercrime investigation where digital evidence preservation determines case outcomes.[46]

Section 173 revolutionizes complaint filing procedures by enabling electronic submission of First Information Reports. Victims of cognizable offenses can now file complaints through electronic means without visiting police stations physically. This provision reduces administrative burdens and ensures prompt registration of cybercrime complaints. The electronic filing system particularly benefits victims of online harassment, financial frauds, and digital stalking who may prefer remote reporting mechanisms. The provision also facilitates faster response times for time-sensitive cybercrime investigations.[47]

Electronic communication provisions under BNSS transform traditional procedural requirements through digital integration. Section 94 empowers courts and police to seize electronic communications and devices containing digital evidence. This provision specifically targets cybercrime investigations where electronic devices constitute primary evidence sources. The legislation permits electronic service of summons, warrants, and notices through digital communication channels. These reforms eliminate delays traditionally associated with physical service of legal documents in cybercrime cases.[48]

[45] Bharatiya Nagarik Suraksha Sanhita 2023, s 105
[46] Bharatiya Nagarik Suraksha Sanhita 2023, s 176(3)
[47] 'Criminal justice system enters the digital age' (Law.asia, 8 April 2025) https://law.asia/bnss-criminal-justice-reforms accessed 30 May 2025
[48] 'Stringent measures against cybercrimes in India's new criminal justice system' (JSA Law, 17 July 2024) https://www.jsalaw.com/newsletters-and-updates/stringent-measures-against-cybercrimes-in-indias-new-criminal-justice-system accessed 30 May 2025

Section 532 enables conducting trials, inquiries, and proceedings through electronic mode using audio-video communication technology. This provision allows remote participation of witnesses, accused persons, and legal representatives in judicial proceedings. The electronic trial framework proves particularly beneficial for cybercrime cases involving multiple jurisdictions or international cooperation. Virtual proceedings also protect vulnerable witnesses in cases involving cyber harassment, stalking, or exploitation. The provision ensures continuity of judicial processes during emergencies or special circumstances.[49]

The BNSS introduces comprehensive provisions for electronic evidence management through Section 231 which permits electronic access to case documents. Statements, confessions, and other materials can be provided to accused persons electronically in sessions court cases. This digital documentation system reduces paperwork, minimizes errors, and improves accessibility for all parties. The electronic access provision particularly benefits complex cybercrime cases involving voluminous digital evidence requiring frequent reference during proceedings.[50]

Section 80 of BNSS specifically addresses witness examination through audio-video electronic means enhancing convenience and accuracy. This provision enables remote testimony which proves crucial in cybercrime cases where witnesses may be located across different geographical jurisdictions. The audio-video examination system also protects witnesses from intimidation or coercion particularly relevant in cases involving organized cybercrime syndicates. The recorded testimonies create permanent records reducing disputes over witness statements.[51]

F. Banking and Financial Services Sector

The banking and financial services sector remains the most targeted domain for cybercriminal activities in India. The Reserve Bank of India has established comprehensive cybersecurity frameworks to address sector-specific vulnerabilities. The RBI Cyber Security Framework for Banks, 2016 mandates all scheduled commercial banks to implement board-approved

[49] Bharatiya Nagarik Suraksha Sanhita 2023, s 532
[50] 'Use Of Audio-Video Electronic Means For Investigation & Trial According To BNSS' (LiveLaw, 15 January 2024) https://www.livelaw.in/top-stories/use-of-audio-video-electronic-means-for-investigation-trial-according-to-bnss-246726 accessed 30 May 2025
[51] 'Revolutionising digital forensics: India's new legal frontiers' (Bar and Bench, 27 July 2024) https://www.barandbench.com/columns/revolutionizing-digital-forensics-indias-new-legal-frontiers accessed 30 May 2025

cybersecurity policies.[52] These policies must encompass network security, access controls, incident response mechanisms and data loss prevention protocols. Banks are required to report cybersecurity incidents to the RBI within specified timeframes ranging from two to six hours after detection. The Master Direction on Information Technology Governance, Risk Controls and Assurance Practices, 2023 further strengthens governance requirements for financial institutions.[53] These directives establish robust risk management frameworks specifically addressing digital banking vulnerabilities including mobile banking, internet banking and payment gateway security.

The Information Technology Framework for Non-Banking Financial Companies focuses on cybersecurity measures for NBFCs engaging in digital financial services. This framework mandates implementation of multi-factor authentication systems, encryption protocols and regular security audits.[54] Financial institutions must also comply with data localization requirements ensuring sensitive customer data remains within Indian jurisdiction. Despite comprehensive regulatory frameworks, enforcement challenges persist across the banking sector. The absence of specialized cybercrime investigation units within banking regulators hampers effective incident response. Moreover, cross-border nature of financial cybercrimes creates jurisdictional complications requiring enhanced international cooperation mechanisms.[55]

JUDICIAL INTERPRETATION AND CASE LAW ANALYSIS

Indian courts have played a transformative role in shaping cybercrime jurisprudence through landmark judgments. These judicial decisions established foundational principles for addressing digital age offenses. The evolution of case law demonstrates progressive judicial thinking in confronting technological challenges.

[52] Reserve Bank of India, 'Cyber Security Framework in Banks' (RBI 2016) https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=10435 accessed 30 May 2025

[53] Reserve Bank of India, 'Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices' (RBI 2023) https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12207 accessed 30 May 2025

[54] Reserve Bank of India, 'Information Technology Framework for NBFC Sector' (RBI 2017) https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=11142 accessed 30 May 2025

[55] Tejashwini K.C., 'Cyber Crime in India with Reference to Banking Sector' (2023) ResearchGate https://www.researchgate.net/publication/372139036_CYBER_CRIME_IN_INDIA_WITH_REFERENCE_TO_BANKING_SECTOR accessed 30 May 2025

A. Shreya Singhal v. Union of India: Redefining Digital Free Speech

The Shreya Singhal case represents the most significant cybercrime judgment in Indian legal history. This 2015 Supreme Court decision fundamentally altered the landscape of online speech regulation. The case arose from arrests under Section 66A of "The Information Technology Act, 2000".[56] Mumbai Police arrested two women for posting allegedly offensive Facebook comments following Bal Thackeray's death. The arrests triggered nationwide protests against arbitrary application of cybercrime provisions. Civil society organizations challenged the constitutional validity of Section 66A through multiple petitions.

A two-judge bench comprising Justices Chelameswar and Nariman delivered the unanimous verdict. The Court declared Section 66A unconstitutional for violating Article 19(1)(a) guaranteeing freedom of speech. The provision was struck down as vague, overbroad and arbitrarily implemented.[57] The judgment established crucial principles for online speech regulation. Terms like "grossly offensive," "annoying," and "inconvenient" were deemed constitutionally impermissible for their vagueness. The Court emphasized that chilling effect on free speech cannot be tolerated in democratic societies.[58] The decision also clarified intermediary liability under Section 79 requiring court orders for content removal.

B. K.S. Puttaswamy v. Union of India: Privacy in Digital Age

The Puttaswamy verdict recognized "privacy as a fundamental right with profound implications for cybercrime law. A nine-judge bench unanimously held that privacy forms an intrinsic part of Article 21. This decision fundamentally altered the constitutional framework for addressing cyber threats."[59] Justice K.S. Puttaswamy challenged the Aadhaar scheme's constitutional validity citing privacy violations. The case questioned whether massive biometric data collection violated individual rights. Government argued that Indian Constitution did not explicitly guarantee privacy protection.

The Supreme Court overruled previous decisions denying constitutional protection to privacy

[56] 'Shreya Singhal v. Union of India' Global Freedom of Expression https://globalfreedomofexpression.columbia.edu/cases/shreya-singhal-v-union-of-india/ accessed 30 May 2025
[57] 'The case of Shreya Singhal Vs Union of India' Jyoti Judiciary https://www.jyotijudiciary.com/the-case-of-shreya-singhal-vs-union-of-india/ accessed 30 May 2025
[58] Shreya Singhal v Union Of India Casemine https://www.casemine.com/judgement/in/5790b244e561097e45a4e264 accessed 30 May 2025
[59] Justice K.S. Puttaswamy (Retd.) & Anr. vs Union of India & Ors. (2017) 10 SCC 1

rights. Justice Chandrachud authored the plurality opinion emphasizing privacy as essential for human dignity. The Court established that any privacy invasion must satisfy tests of legality, necessity and proportionality.[60] This judgment provides crucial framework for evaluating cybercrime investigations involving personal data. Law enforcement agencies must now justify digital surveillance measures more rigorously. The decision influences how courts interpret search and seizure provisions in cybercrime cases.[61]

C. State of Tamil Nadu v. Suhas Katti: Pioneer Cybercrime Conviction

The Suhas Katti case achieved historical significance as India's first cybercrime conviction under IT Act provisions. This 2004 Chennai court decision established important precedents for prosecuting online harassment. The case demonstrated effective enforcement of nascent cybercrime legislation.[62] Accused Suhas Katti created fake profiles to harass a woman through Yahoo Groups after she rejected his marriage proposal. He posted obscene messages and circulated defamatory content damaging her reputation. The victim filed complaints under Sections 67, 469, and 509 of respective Acts.[63]

The Additional Chief Metropolitan Magistrate convicted Katti under multiple provisions. He received two years rigorous imprisonment and Rs. 4,000 fine under Section 67 IT Act. Additional sentences were imposed under IPC sections for forgery and outraging women's modesty.[64] The case established several important legal principles for cybercrime prosecution. "Electronic evidence under Section 65B of Evidence Act was admitted for the first time." The court recognized private experts' role in digital forensics analysis. Forgery of electronic documents was recognized as criminal offense under IPC provisions.

D. Anuradha Bhasin v. Union of India: Internet Access as Fundamental Right

The Anuradha Bhasin judgment addressed internet shutdowns' constitutionality in Jammu and

[60] 'Justice K.S. Puttaswamy v Union of India' Supreme Court Observer https://www.scobserver.in/cases/puttaswamy-v-union-of-india-fundamental-right-to-privacy-case-background/ accessed 30 May 2025

[61] 'KS Puttaswamy v. Union of India: Landmark Case on Right to Privacy' LawCtopus https://www.lawctopus.com/clatalogue/clat-pg/ks-puttaswamy-v-union-of-india/ accessed 30 May 2025

[62] State of Tamil Nadu vs Suhas Katti CC No. 4680 of 2004

[63] 'State of Tamil Nadu vs Suhas Katti, 2004 - Detailed Case Analysis' Testbook https://testbook.com/landmark-judgements/state-of-tamil-nadu-vs-suhas-katti accessed 30 May 2025

[64] 'Case Summary : State of Tamil Nadu Vs Suhas Katti' E-Justice India https://www.ejusticeindia.com/case-summary-state-of-tamil-nadu-vs-suhas-katti-cyber-law-case-in-india/ accessed 30 May 2025

Kashmir. This 2020 Supreme Court decision recognized internet access as fundamental right under Article 19. The case established important safeguards against arbitrary digital restrictions.[65] Following Article 370's revocation, government imposed complete internet shutdown in Kashmir region. Anuradha Bhasin, executive editor of Kashmir Times, challenged these restrictions citing constitutional violations. The petition argued that internet access was essential for exercising fundamental rights.[66]

Justice Ramana-led bench held that indefinite internet suspension violates constitutional principles. The Court applied proportionality test requiring legitimate aims and least restrictive means. Government orders restricting internet access must be published and subject to judicial review.[67] The judgment recognized freedom of speech and trade through internet as constitutionally protected rights. However, the Court balanced these rights against legitimate security concerns in Kashmir. The decision provides framework for challenging future internet shutdowns across India.[68]

E. Avnish Bajaj v. State: Intermediary Liability Evolution

The Avnish Bajaj case examined intermediary liability for third-party content before safe harbor provisions existed. This 2005 Delhi High Court decision influenced subsequent amendments to IT Act provisions. The case highlighted complex issues surrounding platform responsibility for user-generated content.[69] An IIT student listed obscene MMS video for sale on Bazee.com platform. Delhi Police arrested CEO Avnish Bajaj under Section 67 IT Act despite company's lack of direct involvement. The case raised fundamental questions about corporate criminal liability in cyberspace.[70]

Delhi High Court distinguished between company liability and director's personal responsibility. The Court held that "prima facie case existed against Bajaj under Section 85 IT

[65] Anuradha Bhasin v Union of India 2020 SCC OnLine SC 25
[66] 'Anuradha Bhasin v. Union of India: Legality of Internet Shutdown' LawCtopus https://www.lawctopus.com/clatalogue/clat-pg/anuradha-bhasin-v-union-of-india-internet-shutdown/ accessed 30 May 2025
[67] 'Case Brief: Anuradha Bhasin v Union of India' LawBhoomi https://lawbhoomi.com/case-brief-anuradha-bhasin-v-union-of-india/ accessed 30 May 2025
[68] 'Internet Shutdowns and Their Ramifications' Drishti IAS https://www.drishtiias.com/daily-updates/daily-news-editorials/internet-shutdowns-and-their-ramifications accessed 30 May 2025
[69] Avnish Bajaj vs State (N.C.T.) Of Delhi (2005) 3 CompLJ 364 Del
[70] 'Avnish Bajaj vs State (Bazee.com case)' IT Law https://www.itlaw.in/avnish-bajaj-vs-state/ accessed 30 May 2025

Act. However, Indian Penal Code did not recognize automatic director liability when company wasn't arraigned."[71] This judgment catalyzed introduction of Section 79 safe harbor provisions in 2008 IT Act amendments. The case demonstrated need for clearer intermediary liability frameworks. Subsequent legislative changes provided greater protection for platforms against third-party content liability.[72]

COMPARATIVE ANALYSIS: INTERNATIONAL BEST PRACTICES

A. European Union: GDPR and Cybersecurity Framework

The European Union's General Data Protection Regulation represents the gold standard for comprehensive data protection legislation globally. The GDPR's extraterritorial reach ensures uniform data protection standards for all organizations processing EU residents' personal data regardless of geographical location.[73] This comprehensive approach contrasts sharply with India's sectoral regulatory framework that creates compliance gaps across different industries. "The GDPR's risk-based approach to data protection mandates organizations to conduct Data Protection Impact Assessments for high-risk processing activities. These assessments help identify potential privacy risks and implement appropriate safeguards before data processing commences."[74] India's Information Technology Act lacks similar proactive risk assessment requirements, focusing primarily on post-incident penalties rather than preventive measures.

"The EU's Network and Information Security Directive establishes comprehensive cybersecurity requirements for critical infrastructure operators and digital service providers." This directive mandates incident reporting, risk management measures and security standards across essential services.[75] The directive's sectoral approach provides valuable lessons for India's critical information infrastructure protection framework. European enforcement

[71] 'Avnish Bajaj vs. State (DPS MMS Scandal Case)' Indian Case Law https://indiancaselaw.in/avnish-bajaj-vs-state-dps-mms-scandal-case/ accessed 30 May 2025

[72] Avnish Bajaj vs State on 29 May, 2008 Indian Kanoon https://indiankanoon.org/doc/309722/ accessed 30 May 2025

[73] Michael Edwards, 'Comparative Analysis of Data Protection Laws: EU, US, and Asia' (1 October 2024) https://michaeledwards.uk/comparative-analysis-of-data-protection-laws-eu-us-and-asia/

[74] 'Data Privacy Laws and Compliance: A Comparative Review of the EU GDPR and USA Regulations' Academia.edu (9 March 2024) https://www.academia.edu/125369936/Data_Privacy_Laws_and_Compliance_A_Comparative_Review_of_the_Eu_GDPR_and_Usa_Regulations

[75] 'GDPR's Impact on Cybersecurity: A Review Focusing on USA and European Practices' ResearchGate (9 February 2024) https://www.researchgate.net/publication/378106122_GDPR's_impact_on_cybersecurity_A_review_focusing_on_USA_and_European_practices

mechanisms demonstrate effective regulatory coordination with substantial financial penalties reaching up to 4% of annual global turnover for GDPR violations. The consistency of enforcement across EU member states contrasts with India's fragmented enforcement landscape involving multiple regulatory agencies.[76]

B. United States: Sectoral Approach and Federal Coordination

The United States employs a sectoral approach to cybersecurity regulation with specialized frameworks for different industries. The Health Insurance Portability and Accountability Act governs healthcare data protection while the Gramm-Leach-Bliley Act addresses financial services cybersecurity.[77] This sectoral specialization allows for industry-specific requirements tailored to unique operational contexts. The Cybersecurity and Infrastructure Security Agency coordinates federal cybersecurity efforts and provides guidance to critical infrastructure operators. CISA's role in facilitating information sharing between government and private sector demonstrates effective public-private partnership models.[78] India's Computer Emergency Response Team could benefit from similar coordination mechanisms and enhanced private sector engagement.

The US approach to breach notification requirements varies significantly across states creating compliance complexities for multi-state operations. However, this diversity also allows for regulatory experimentation and identification of best practices.[79] The California Consumer Privacy Act serves as a model for comprehensive state-level privacy legislation that influenced subsequent federal proposals. Federal agencies like the Federal Trade Commission employ broad consumer protection authorities to address cybersecurity violations even without specific cybersecurity mandates. This flexible enforcement approach enables rapid response to emerging threats without requiring lengthy legislative processes.[80]

---

[76] 'Comparative Analysis of Data Protection Laws: Learning from Global Best Practices' ResearchGate (5 October 2024) https://www.researchgate.net/publication/385139126_Comparative_Analysis_of_Data_Protection_Laws_Learning_from_Global_Best_Practices

[77] Ruben de Bruin, 'A Comparative Analysis of the EU and U.S. Data Privacy Regimes' SSRN (18 October 2022) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4251540

[78] 'Attributes Impacting Cybersecurity Policy Development: An Evidence from Seven Nations' ScienceDirect https://www.sciencedirect.com/science/article/pii/S0167404822002140

[79] 'A Comparative Analysis of the EU GDPR to the US's Breach Notifications' Taylor & Francis Online https://www.tandfonline.com/doi/abs/10.1080/13600834.2019.1571473

[80] 'Cybercrime Comparison Under Criminal Law in Some Countries' Academia.edu (1 January 2018) https://www.academia.edu/127357946/Cybercrime_Comparison_Under_Criminal_Law_in_Some_Countries

C. Singapore: Integrated Regulatory Framework

Singapore's integrated approach to cybersecurity and data protection provides a comprehensive model for developing economies. The Personal Data Protection Act, 2012 establishes uniform data protection standards while the Cybersecurity Act, 2018 addresses critical infrastructure protection.[81] This dual-track approach ensures comprehensive coverage without regulatory gaps. The Personal Data Protection Commission's guidance documents provide clear implementation roadmaps for organizations across different sectors. These guidance materials help bridge the gap between legal requirements and practical implementation challenges.[82] Singapore's emphasis on regulatory clarity and practical guidance offers valuable lessons for improving India's regulatory communication.

Singapore's approach to critical information infrastructure protection designates specific sectors including banking, healthcare, telecommunications and government systems. The Cybersecurity Act mandates proactive security measures, regular audits and incident reporting requirements.[83] This comprehensive framework provides a model for strengthening India's critical infrastructure protection mechanisms. The integration of cybersecurity and data protection enforcement under unified regulatory oversight ensures consistent application of security standards. Singapore's Personal Data Protection Commission works closely with the Cyber Security Agency to address overlapping regulatory concerns.

RECOMMENDATIONS & CONCLUSION

India's cybercrime legal framework requires comprehensive transformation to address contemporary digital challenges effectively. The existing Information Technology Act, 2000 demonstrates structural inadequacies in combating sophisticated cyber threats. Legislative modernization through substantive amendments represents an urgent national priority for digital security enhancement.[84] The proposed Digital India Act, 2023 offers promising

[81] CMS Expert Guide, 'Data Protection and Cybersecurity Laws in Singapore' (19 March 2025) https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/singapore

[82] Securiti, 'Singapore's Data Privacy and Cybersecurity Landscape' (8 August 2024) https://securiti.ai/whitepapers/singapore-data-privacy-and-cybersecurity-overview/

[83] Cyber Security Agency of Singapore, 'Cybersecurity Act' https://www.csa.gov.sg/legislation/cybersecurity-act

[84] Vinay K, 'Challenges Faced by Law Enforcement Agencies in Investigating and Prosecuting Cyber Crimes in India' (2024) ResearchGate https://www.researchgate.net/publication/383785171_CHALLENGES_FACED_BY_LAW_ENFORCEMENT_AGENCIES_IN_INVESTIGATING_AND_PROSECUTING_CYBER_CRIMES_IN_INDIA accessed 30 May 2025

solutions for addressing emerging technology challenges. This future-ready legislation incorporates provisions for artificial intelligence regulation, deepfake prevention, and blockchain governance mechanisms. However, implementation requires careful consideration of constitutional safeguards and international cooperation frameworks.[85] The Act's emphasis on algorithmic transparency and automated decision-making accountability aligns with global best practices.

Specialized cybercrime courts establishment emerges as a critical reform recommendation for India's judicial infrastructure. These dedicated tribunals should possess technical expertise and fast-track procedures for complex digital offenses. Judicial training programs must emphasize digital evidence collection, preservation standards, and cross-border investigation techniques.[86] The creation of cyber forensic laboratories in every state becomes essential for evidence authentication and criminal prosecution support.

Law enforcement capacity building represents another fundamental reform priority requiring sustained government investment. Specialized cybercrime investigation units need establishment within state police departments nationwide. Technical training programs should focus on dark web investigations, cryptocurrency tracing, and advanced persistent threat analysis.[87] Public-private partnerships facilitate knowledge sharing between security researchers and law enforcement agencies effectively. Data protection framework integration with cybercrime legislation ensures comprehensive digital rights protection mechanisms.

Constitutional compliance remains paramount throughout cybercrime law reform processes within India's legal system. The Supreme Court's judgment in Shreya Singhal v. Union of India establishes important precedents for online speech regulation. Future legislation must respect fundamental rights while providing adequate law enforcement tools.[88] Proportionality principles should guide surveillance powers and evidence collection procedures consistently. Technology-neutral legislation design ensures legal framework adaptability to future

[85] Ministry of Electronics and Information Technology, 'Digital India Act 2023 Consultation Paper' (Government of India 2023) https://www.drishtiias.com/daily-updates/daily-news-editorials/india-s-digital-future-the-digital-india-act-2023

[86] Legal Service India, 'Need for Police Reforms in India Police Reforms vis-a-vis Cyber Crimes' (Legal Resources) https://www.legalserviceindia.com/legal/article-388-need-for-police-reforms-in-india-police-reforms-vis-a-vis-cyber-crimes.html accessed 30 May 2025

[87] International Journal of Law Management & Humanities, 'A Study on Cyber Crime and its Legal Framework in India' (IJLMH 2022) https://ijlmh.com/paper/a-study-on-cyber-crime-and-its-legal-framework-in-india/ accessed 30 May 2025

[88] Shreya Singhal v Union of India (2015) 5 SCC 1

technological developments and innovations. Principle-based regulatory approaches accommodate rapid technological evolution. Regular legislative reviews must incorporate stakeholder feedback and emerging threat assessments for continuous improvement.[89]

[89] Lawctopus, 'Indian Legal System In Dealing With Cybercrime' (4 August 2024) https://www.lawctopus.com/academike/indian-legal-system-cybercrime/ accessed 30 May 2025

BIBLIOGRAPHY

A. Primary Sources

1. Legislation

- Information Technology Act 2000 (India)
- Indian Penal Code 1860
- Digital Personal Data Protection Act 2023 (India)
- Bharatiya Nyaya Sanhita 2023

2. International Instruments

- Convention on Cybercrime (Budapest Convention) 2001, ETS 185
- United Nations Convention against Cybercrime 2024
- Additional Protocol to the Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence 2022, ETS 224
- United Nations Convention against Transnational Organized Crime 2000

B. Secondary Sources

1. Books & Journal Articles

- Sharma V, Information Technology Law and Practice- Cyber Laws and Laws Relating to E-Commerce (5th edn, Universal Law Publishing 2016)
- Curtis J and Oxburgh G, Understanding cybercrime in 'real world' policing and law enforcement (Sage Publications 2023)
- Atrey I, 'Cybercrime and its Legal Implications: Analysing the challenges and Legal frameworks surrounding Cybercrime, including issues related to

Jurisdiction, Privacy, and Digital Evidence' (2023) 10(3) International Journal of Research and Analytical Reviews

- 'A systematic literature review on cybercrime legislation' PMC National Center for Biotechnology Information https://pmc.ncbi.nlm.nih.gov/articles/PMC11384205/

- 'A Study on Cyber Crime and its Legal Framework in India' (2022) International Journal of Law Management & Humanities https://ijlmh.com/paper/a-study-on-cyber-crime-and-its-legal-framework-in-india/

- Vinay K, 'Challenges Faced by Law Enforcement Agencies in Investigating and Prosecuting Cyber Crimes in India' (ResearchGate, April 2024) https://www.researchgate.net/publication/383785171_CHALLENGES_FACED_BY_LAW_ENFORCEMENT_AGENCIES_IN_INVESTIGATING_AND_PROSECUTING_CYBER_CRIMES_IN_INDIA

- 'Emerging Technologies and Future Challenges in Indian Cyber Law' (ResearchGate, January 2024) https://www.researchgate.net/publication/377473599_EMERGING_TECHNOLOGIES_AND_FUTURE_CHALLENGES_IN_INDIAN_CYBER_LAW

C. Online Sources

1. News Articles and Legal Resources

- 'India's Digital Future: The Digital India Act 2023' Drishti IAS (9 October 2023) https://www.drishtiias.com/daily-updates/daily-news-editorials/india-s-digital-future-the-digital-india-act-2023

- 'Tackling cybercrime: Greater digitisation leads to rising challenges' Law.Asia (7 November 2024) https://law.asia/india-cybersecurity-legislation-reform/

- 'Explained: The Digital India Act 2023' Vidhi Legal Policy (8 August 2023) https://vidhilegalpolicy.in/blog/explained-the-digital-india-act-2023/

- 'Need for Police Reforms in India Police Reforms vis-a-vis Cyber Crimes' Legal Service India https://www.legalserviceindia.com/legal/article-388-need-for-police-reforms-in-india-police-reforms-vis-a-vis-cyber-crimes.html

- 'Indian Legal System In Dealing With Cybercrime' Lawctopus (4 August 2024) https://www.lawctopus.com/academike/indian-legal-system-cybercrime/

- 'IT Act 2000: Objectives, Features, Amendments, Sections, Offences and Penalties' ClearTax (12 April 2024) https://cleartax.in/s/it-act-2000