Page: 1009-1046 *URL: www.lijdlr.com*

LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

ISSN: 2583-7753

LawFoyer International Journal of Doctrinal Legal Research

[ISSN: 2583-7753]

Volume 4 | Issue 4

2026

DOI: https://doi.org/10.70183/lijdlr.2026.v04.412

© 2026 LawFoyer International Journal of Doctrinal Legal Research

Follow this and additional research works at: www.lijdlr.com
Under the Platform of LawFoyer – www.lawfoyer.in

After careful consideration, the editorial board of LawFoyer International Journal of Doctrinal Legal Research has decided to publish this submission as part of the publication.

In case of any suggestions or complaints, kindly contact (info.lijdlr@gmail.com)
To submit your Manuscript for Publication in the LawFoyer International Journal of Doctrinal Legal Research, To submit your Manuscript Click here

CYBER CRIME WITHIN THE INDIAN LEGAL FRAMEWORK: TYPOLOGY, STATUTORY ARCHITECTURE AND JUDICIAL RESPONSE IN THE ERA OF THE BHARATIYA NYAYA SANHITA, 2023

Abhishek Anand[1]

I. ABSTRACT

India recorded 1,01,928 cyber-crime cases in 2024, the first year in which such registrations crossed one lakh, even as overall cognisable crime declined. This article examines whether India's legal framework is equipped to meet that trajectory. Existing scholarship rarely maps offences against both special and general penal law, has scarcely absorbed the new criminal codes, and treats enforcement as peripheral. Using doctrinal and analytical methods, the article first constructs a typology of twenty prevalent forms of cyber crime, grouped into five functional clusters, and maps each against the Information Technology Act, 2000, the Indian Penal Code, 1860 and its successor, the Bharatiya Nyaya Sanhita, 2023, and allied special statutes. It then traces the statutory architecture from the UNCITRAL Model Law to the 2008 amendments, the Intermediary Rules of 2021 and their 2026 amendment on synthetically generated information, the Digital Personal Data Protection Act, 2023, and the three new criminal codes. Thirdly, it evaluates the judicial response across six doctrinal fields: early prosecutions, domain names and phishing, obscenity and speech, intermediary liability, privacy and surveillance, and electronic evidence. The article argues that the framework is substantively broad but structurally fragmented: offences are scattered across overlapping statutes, key terms remain undefined, and several harmful practices fall outside penal law. Enforcement lags far behind registration: fraud drove 72.6 per cent of the 2024 cases, Karnataka charge-sheeted only 18.1 per cent of its cases in 2023, and about 1.2 lakh cases awaited investigation at the end of 2024. The IT Act–BNS overlap also remains unresolved, because courts settle it only offence by offence. The article

[1] Phd Student, University of Delhi (India). Email: abhishekanandmishra13@gmail.com.

concludes with targeted reform proposals, including a statutory definition and consolidated offence schedule, an express resolution of the IT Act–BNS overlap, gender-neutral cyberstalking provisions, and investment in investigative and cross-border capacity.

II. KEYWORDS

Cyber-crime; Information Technology Act, 2000; Bharatiya Nyaya Sanhita, 2023; intermediary liability; cyber fraud.

III. INTRODUCTION

A. Research Problem

The digitisation of Indian economic and social life has been accompanied by an equally rapid digitisation of crime. According to the National Crime Records Bureau (NCRB), cyber crime registrations rose from 65,893 cases in 2022 to 86,420 in 2023, an increase of 31.2 per cent.[2] In 2024, registrations crossed one lakh for the first time, reaching 1,01,928, a further increase of 17.9 per cent, even as total cognisable crime fell by roughly six per cent; fraud was the motive in 73,987 of these cases, or 72.6 per cent.[3] The Supreme Court has recently had to take suo motu cognisance of "digital arrest" scams in which offenders impersonate police, investigative agencies and even the Court itself.[4]

These numbers pose a direct question for legal scholarship: is the Indian legal framework adequate to the forms that cyber crime now takes? The question is more pressing because the framework itself has changed significantly. On 1 July 2024 the

---

[2]NAT'L CRIME RECORDS BUREAU, MINISTRY OF HOME AFFS., CRIME IN INDIA 2023, tbl. 9A.1 (2025); *see also Cybercrime Soars by 31% in India, Karnataka Tops with 21,889 Cases*, NEWS MINUTE (Sept. 30, 2025), https://www.thenewsminute.com/news/cybercrime-soars-by-31-in-india-karnataka-tops-with-21889-cases.

[3]NAT'L CRIME RECORDS BUREAU, MINISTRY OF HOME AFFS., CRIME IN INDIA 2024, tbls. 9A.1, 9A.3 (2026) (registrations by State and by motive); *see also Bengaluru Records 17,561 Cybercrime Cases in 2024, Highest Among Metro Cities Again*, NEWS MINUTE (May 2026), https://www.thenewsminute.com/karnataka/bengaluru-records-17561-cybercrime-cases-in-2024-highest-among-metro-cities-again.

[4]*In re* Victims of Digital Arrest Related to Forged Documents, Suo Motu Writ Petition (Crl.) No. 3 of 2025 (SC Dec. 1, 2025) (India) (directing the Central Bureau of Investigation to act as the primary investigating agency).

Indian Penal Code, 1860 (IPC), the Code of Criminal Procedure, 1973 and the Indian Evidence Act, 1872 were replaced by the Bharatiya Nyaya Sanhita, 2023 (BNS), the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS) and the Bharatiya Sakshya Adhiniyam, 2023 (BSA).[5] The Digital Personal Data Protection Rules, 2025 were notified in November 2025, bringing the Digital Personal Data Protection Act, 2023 into force in phases,[6] and the intermediary rules were amended in February 2026 to address synthetically generated content.[7] Much of the existing literature on Indian cyber law predates these changes and remains anchored to IPC provisions that no longer operate prospectively.

The existing literature falls broadly into three groups. Treatise-style works catalogue offences and the IT Act provisions that address them;[8] journal studies survey judicial decisions and argue for greater judicial activism;[9] and policy commentary concentrates on intermediary regulation and free speech after *Shreya Singhal v. Union of India*. Three gaps follow. Few studies map offences systematically against both the IT Act and the general penal code; almost none have yet absorbed the replacement of the IPC by the BNS; and the institutional question of whether registered cases are actually investigated and prosecuted is usually treated as peripheral, when the data suggest it is central. This article seeks to address all three.

---

[5]The Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023 (India) [hereinafter BNS]; The Bharatiya Nagarik Suraksha Sanhita, 2023, No. 46, Acts of Parliament, 2023 (India) [hereinafter BNSS]; The Bharatiya Sakshya Adhiniyam, 2023, No. 47, Acts of Parliament, 2023 (India) [hereinafter BSA].

[6]The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India) [hereinafter DPDP Act]; Digital Personal Data Protection Rules, 2025, G.S.R. 846(E) (Nov. 13, 2025) (India); Ministry of Elecs. & Info. Tech., Notification G.S.R. 843(E) (Nov. 13, 2025) (India) (bringing the provisions on the Data Protection Board into force on Nov. 13, 2025, the consent manager provisions in sections 6(9) and 27(1)(d) on Nov. 13, 2026, and the remaining provisions, including the duties of data fiduciaries and the penalty provisions, on May 13, 2027). No later Gazette notification altering this schedule had been published as of Nov. 24, 2026.

[7]Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, G.S.R. 120(E) (Feb. 10, 2026) (India).

[8]*See, e.g.*, PRASHANT MALI, CYBER LAW & CYBER CRIMES (2012); G.S. BAJPAI, ON CYBER CRIME & CYBER LAW (2011); FAROOQ AHMAD, CYBER LAW IN INDIA (LAW ON INTERNET) (3d ed. 2008).

[9]*See, e.g.*, Abhijeet Deb, *Cyber Crime and Judicial Response in India*, 3 INDIAN J.L. & JUST. 106 (2012); V.M. Eshwar & Aswathy Rajan, *A Critical Analysis on Judicial Activism in Relation to Cyber Law – An Indian Perspective*, 119 INT'L J. PURE & APPLIED MATHEMATICS 1489 (2018).

B. Research Objectives

The article pursues three objectives: first, to map the principal forms of cyber crime prevalent in India against the provisions of the IT Act, the BNS and allied special statutes that now govern them; secondly, to trace the evolution and present organisation of the statutory architecture, from the UNCITRAL Model Law to the new criminal codes, the DPDP Act and the amended intermediary rules; and thirdly, to evaluate the judicial and institutional response and to identify the doctrinal and enforcement gaps that call for reform.

C. Research Questions

This article addresses three research questions.

First, what are the principal forms of cyber crime prevalent in India, and how is each treated by the law as it now stands?

Secondly, how is the statutory architecture organised, and how has it evolved?

Thirdly, how have Indian courts responded, and where do doctrinal and institutional gaps remain?

D. Research Methodology

The method is doctrinal and analytical. The primary sources are the IT Act, the BNS, the BNSS, the BSA, the DPDP Act and allied special statutes; subordinate legislation, including the intermediary rules and the DPDP Rules; and judgments of the Supreme Court and the High Courts. The NCRB's *Crime in India* reports for 2022 to 2024 and the regulatory instruments of the Reserve Bank of India and CERT-In supply the empirical base, and secondary literature informs the analysis. The study covers the period from the enactment of the IT Act in 2000 to November 2026, and the law is stated as on 24 November 2026. It is limited to substantive and procedural criminal law and its immediate regulatory surroundings; it does not address cyber security standards for critical infrastructure in detail.

Part II sets out the conceptual frame. Part III presents a typology of twenty forms of cyber crime in five clusters and maps each to its governing provisions. Part IV examines the statutory architecture. Part V analyses the judicial response. Part VI

offers a critical appraisal, and Part VII sets out suggestions and recommendations. Part VIII concludes, and a consolidated list of references follows.

IV. CONCEPTUALISING CYBER CRIME

No Indian statute defines "cyber crime." The Information Technology Act, 2000 (IT Act) defines a "computer," "computer network," "computer resource" and "data," but organises its offences around conduct rather than around any general concept.[10] The BNS goes further in one respect, listing "cyber-crimes" among the activities that can constitute organised crime under section 111, yet it too leaves the term undefined.[11] The definitional gap matters, because a term that carries enhanced punishment in one provision and has no settled meaning elsewhere invites inconsistent charging.

The literature commonly approaches cyber crime through the role played by the computer. In the first category the computer is the *target*, as in hacking, denial-of-service attacks or the release of malicious code. In the second it is the *instrument*, as in online fraud, phishing or cyber defamation, where a conventional wrong is committed through digital means. In the third it is *incidental*, holding evidence of an offence committed offline.[12] A related distinction, now standard in comparative criminology, separates *cyber-dependent* crimes, which cannot exist without information and communication technology, from *cyber-enabled* crimes, which are traditional offences whose scale or reach is transformed by it. The distinction has practical consequences in India. Cyber-dependent crimes fall mainly under the IT Act, while cyber-enabled crimes are prosecuted largely under the general penal code, and the interaction between the two is where much of the doctrinal friction lies.

Two features of cyber crime complicate the application of conventional criminal-law concepts. The first is attribution. An offence may be routed through compromised machines, anonymising networks and accounts opened with stolen or purchased

[10]The Information Technology Act, 2000, § 2(1)(i), (j), (k), (o), No. 21, Acts of Parliament, 2000 (India) [hereinafter IT Act].
[11]BNS § 111(1).
[12]MALI, *supra* note 8, at 14–18; ASHISH PANDEY, CYBER CRIMES: DETECTION & PREVENTION ¶¶ 4.1–4.3 (2006).

identities, so that the person whose device or account appears in the record is often not the offender. The Ken Haywood episode, discussed below, illustrates how easily an innocent person's connection can be used. The second is territoriality. The offender, the victim, the server and the money may each be in a different jurisdiction, and the conduct may be lawful in some of them. Indian law responds to the second problem through the extraterritorial reach of section 75 of the IT Act and section 1 of the BNS, but responds to the first mainly through the evidentiary rules on electronic records. Both responses are examined below.

International instruments reflect the same structure. The Council of Europe's Budapest Convention organises offences into those against the confidentiality, integrity and availability of computer systems, computer-related offences, content-related offences and copyright-related offences.[13] India never acceded to that Convention, but in September 2026 it signed the United Nations Convention against Cybercrime, adopted by the General Assembly on 24 December 2024 and opened for signature at Hanoi in October 2025.[14] The typology in Part III draws on this functional scheme while preserving the categories familiar to Indian practice.

V. A TYPOLOGY OF CYBER CRIME AND ITS LEGAL TREATMENT

The forms of cyber crime are not closed; new techniques appear faster than statutes can name them. The twenty forms discussed below are those most frequently encountered in Indian practice and literature. They are grouped into five clusters, and Table 1 at the end of this Part maps each form to its governing provisions under the IT Act, the former IPC and the BNS.

A. Offences Against the Confidentiality, Integrity and Availability of Systems

Hacking is unauthorised access to a computer system, network, program or data. It is the paradigm cyber-dependent offence and is addressed by the civil liability provision

[13]Convention on Cybercrime arts. 2–10, Nov. 23, 2001, E.T.S. No. 185.
[14]G.A. Res. 79/243, United Nations Convention against Cybercrime (Dec. 24, 2024); *India Signs UN Convention Against Cybercrime*, MANORAMA YEARBOOK (Sept. 28, 2026), https://www.manoramayearbook.in/current-affairs/india/2026/09/28/india-signs-un-convention-against-cybercrime.html.

in section 43 of the IT Act read with the criminal offence in section 66, which since 2008 requires dishonest or fraudulent intent.[15] The harm can be severe and diffuse. In 2020, for instance, a twenty-two-year-old student from Vadodara was arrested for allegedly breaching the examination portal of the Gujarat Technological University and leaking the data of 1,275 students, reportedly to force the cancellation of online examinations during the pandemic.[16]

Viruses and worms are malicious programs that damage or replicate across systems. A virus attaches itself to a host file, while a worm propagates independently until it exhausts system resources.[17] The Morris worm of 1988 is widely regarded as the first major attack on the internet,[18] and the "Love Bug" of 2000 caused losses estimated at around ten billion dollars worldwide.[19] Introducing a contaminant or virus attracts sections 43(c) and 43(e) read with section 66 of the IT Act.

Denial-of-service (DoS) attacks flood a system with requests so that legitimate users cannot reach it.[20] The coordinated attacks on Estonia's digital infrastructure in 2007, which followed the government's decision to relocate a Soviet-era war memorial, demonstrated their capacity to disrupt an entire state.[21] Section 43(f) read with section 66 applies, and an attack on a protected system or critical information infrastructure may engage section 66F.

Web jacking is the seizure of control over another's website, typically to deface it or to redirect its users.[22] Indian police websites have themselves been targets; the website

---

[15]IT Act §§ 43(a), 66.
[16]*22-Year-Old Student Held for Hacking GTU Portal, Stealing and Leaking Data*, INDIAN EXPRESS (Aug. 20, 2020), https://indianexpress.com/article/india/22-year-old-student-held-for-hacking-gtu-portal-stealing-and-leaking-data-6561971/.
[17]BAJPAI, *supra* note 8, at 135–36.
[18]*The Morris Worm: 30 Years Since First Major Attack on the Internet*, FED. BUREAU OF INVESTIGATION (Nov. 2, 2018), https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218.
[19]Geoff White, *Love Bug's Creator Tracked Down to Repair Shop in Manila*, BBC NEWS (May 3, 2020), https://www.bbc.com/news/technology-52458765.
[20]BAJPAI, *supra* note 8, at 135.
[21]Damien McGuinness, *How a Cyber Attack Transformed Estonia*, BBC NEWS (Apr. 27, 2017), https://www.bbc.com/news/39655415.
[22]Animesh Sarmah, Roshmi Sarmah & Amlan Jyoti Baruah, *A Brief Study on Cyber Crime and Cyber Laws of India*, 4 INT'L RSCH. J. ENG'G & TECH. 1633, 1635 (2017).

of the Maharashtra CID was hacked and defaced in March 2020.[23] Web jacking falls under sections 43 and 66, and section 65 applies where source code is altered.

Data diddling involves altering raw data before a computer processes it and restoring it afterwards, while *salami attacks* involve the repeated deduction of sums so small that no individual victim complains.[24] In the NDMC electricity billing fraud of 1996, a private contractor handling the Council's computerised collections manipulated data files to understate receipts and misappropriated large sums.[25] Both forms attract sections 43(d) and 43(i), read with section 66, of the IT Act; where entrusted property is involved, criminal breach of trust under section 316(5) of the BNS (formerly section 409 of the IPC) is also available.

Internet time theft, the use by an unauthorised person of internet hours paid for by another, is now largely of historical interest but marked an early milestone. In the *Col. Bajwa* case of 2000, the Delhi Police reportedly registered India's first case of theft of internet hours after the victim's login credentials were misused more than two hundred times.[26] The case is said to have exposed the limited technical capacity of investigators at the time. Charging services to another person's account by tampering with or manipulating a computer system now falls under section 43(h), read with section 66.

Data theft and spyware complete the cluster. Data theft is the unauthorised copying or removal of information.[27] In *Just Dial Pvt. Ltd. v. Infomedia 18 Ltd.*, the Delhi High Court in January 2010 granted an ex parte injunction against the operator of askme.in for allegedly copying Just Dial's database, and appointed local commissioners to seize the

---

[23]Gautam S. Mengle, *Maharashtra CID Website Hacked, Defaced*, THE HINDU (Mar. 7, 2020), https://www.thehindu.com/news/cities/mumbai/maharashtra-cid-website-hacked-defaced/article31005341.ece.
[24]BAJPAI, *supra* note 8, at 138; PANDEY, *supra* note 12, ¶ 7.59.
[25]INDIAN AUDIT & ACCTS. DEP'T, FRAUD DETECTION TECHNIQUES & FORENSIC AUDIT vol. II (2020), https://cag.gov.in/uploads/media/Vol-II-Cyber-Crimes-20200528155403.pdf.
[26]PANDEY, *supra* note 12, ¶ 4.3; *Full Guide on Cyber Crimes in India*, INDIA FORENSIC, https://www.indiaforensic.com/compcrime1.htm (last visited July 7, 2021). No first information report, contemporaneous news report or judgment confirming these details has been traced, and the account rests on these secondary sources.
[27]MALI, *supra* note 8, at 14.

storage media concerned.[28] Spyware such as Pegasus, which can be installed remotely and gives the operator control over messages, calls and location data, raises the issue at the level of the state.[29] Unlawful interception or extraction of data attracts sections 43, 66, 66E and 72 of the IT Act; Part V returns to the judicial treatment of the Pegasus allegations.

B. Computer-Related Fraud and Deception

Phishing is the fraudulent acquisition of sensitive information such as passwords or card details by masquerading as a trustworthy entity, and is best understood as a form of social engineering.[30] It is now prosecuted under sections 66C and 66D of the IT Act read with sections 318 and 319 of the BNS, which replaced the cheating provisions in sections 415 to 420 of the IPC.[31] Civil redress is also available. In *Umashankar Sivasubramanian v. ICICI Bank*, the first adjudication under the IT Act, the Adjudicating Officer for Tamil Nadu directed the bank to pay ₹12.85 lakh to a non-resident customer who had lost money to a phishing e-mail, holding the bank responsible for inadequate due diligence.[32]

Internet fraud includes online auction, retail, investment and payment-card frauds. Anonymity, speed and global reach make the internet a congenial environment for such schemes.[33] In the Hotel Le Meridien (Pune) case, a restaurant cashier and three associates cloned the credit cards of about thirty guests and made transactions

---

[28]Just Dial Pvt. Ltd. v. Infomedia 18 Ltd., CS (OS) No. [●] of 2010 (Del. HC Jan. 30, 2010) (India) (ex parte ad-interim order); *Data Theft: HC Asks Askme.in to Shut Down*, ONEINDIA (Jan. 30, 2010), https://www.oneindia.com/2010/01/30/data-theft-hc-asks-askme-in-to-shut-down.html; Eshwar & Rajan, *supra* note 9, at 1493.

[29]Jay Mazoomdaar, *Explained: How Pegasus Spyware Infects a Device; What Data Can Be Compromised*, INDIAN EXPRESS (Aug. 11, 2021), https://indianexpress.com/article/explained/pegasus-whatsapp-spyware-israel-india-7410890/.

[30]MALI, *supra* note 8, at 31–32.

[31]IT Act §§ 66C, 66D; BNS §§ 318, 319.

[32]Umashankar Sivasubramanian v. ICICI Bank, Petition No. 2462 of 2008 (Adjudicating Officer, Tamil Nadu Apr. 12, 2010) (India); *ICICI Bank Told to Pay Rs 13 Lakh to NRI Customer*, ECON. TIMES (Apr. 14, 2010), https://economictimes.indiatimes.com/industry/banking/finance/banking/icici-bank-told-to-pay-rs-13-lakh-to-nri-customer/articleshow/5798944.cms.

[33]Maneela, *Cyber Crimes: The Indian Legal Scenario*, 11 U.S.-CHINA L. REV. 570, 573 (2014).

estimated at nearly ₹1 crore.[34] The contemporary equivalent is the digital arrest and investment scam, in which organised syndicates combine impersonation, intimidation and mule bank accounts. Such frauds attract sections 43 and 66 of the IT Act, section 318 of the BNS and, where a syndicate is involved, section 111 of the BNS.

Identity theft is fraud committed by assuming another's identity.[35] In the 2008 Ahmedabad serial blasts, terrorists used the unsecured Wi-Fi connection of an American resident of Navi Mumbai to send e-mails claiming responsibility.[36] Section 66C of the IT Act and section 319 of the BNS apply.

E-mail spoofing misrepresents the origin of an e-mail, usually to defame or defraud, while *e-mail bombing* floods an inbox or server to disable it.[37] Spoofing is prosecuted under section 66D of the IT Act with sections 318 and 319 of the BNS; bombing under section 43(e) read with section 66.

Digital forgery uses scanners, printers and software to fabricate documents such as cheques, certificates or identity cards.[38] The Abdul Karim Telgi stamp-paper scam remains the leading Indian illustration of the scale such forgery can reach.[39] As enacted, the IT Act amended the IPC through section 91 and the First Schedule so that "electronic records" fell within the forgery provisions. The 2008 amendment omitted sections 91 to 94 and substituted or deleted the original schedules with effect from 27 October 2009, but the changes already made to the IPC continued in force. The BNS now carries that position into section 2(8) and sections 335, 336 and 340.[40]

---

[34]*Hotel Customers Cheated of Rs 1 Cr; Four Held*, TIMES OF INDIA (June 22, 2008), https://timesofindia.indiatimes.com/city/pune/hotel-customers-cheated-of-rs-1-cr-four-held/articleshow/3152968.cms; MALI, *supra* note 8, at 60–61.
[35]MALI, *supra* note 8, at 43–45.
[36]*The Curious Case of Ken Haywood*, INDIAN EXPRESS (Aug. 14, 2008), http://archive.indianexpress.com/news/the-curious-case-of-ken-haywood/348646/.
[37]Sarmah, Sarmah & Baruah, *supra* note 22, at 1634; BAJPAI, *supra* note 8, at 138.
[38]S.K. VERMA & RAMAN MITTAL, LEGAL DIMENSIONS OF CYBER SPACE 235 (2004).
[39]Maneela, *supra* note 33, at 574.
[40]IT Act § 91 & sch. I (as enacted), *omitted by* The Information Technology (Amendment) Act, 2008, § 48, No. 10, Acts of Parliament, 2009 (India) (w.e.f. Oct. 27, 2009); BNS §§ 2(8), 335, 336, 340.

C. Content-Related Offences

Cyber defamation is injury to reputation through online publication. Because a single post can reach a very large audience, the harm can exceed that of print.[41] The first Indian instance is generally said to be *SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra*, in which the Delhi High Court restrained an employee from sending defamatory e-mails about his employer to its subsidiaries and staff.[42] Defamation is now punishable under section 356 of the BNS, which adds community service as an alternative sentence.[43] Section 66A of the IT Act, once invoked against offensive online speech, was struck down in *Shreya Singhal v. Union of India* for vagueness and overbreadth.[44]

Cyber stalking is the repeated harassment or monitoring of a person through electronic communication.[45] The literature often locates it within criminal intimidation, but since 2013 Indian law has addressed it directly. Section 78 of the BNS, which replaces section 354D of the IPC, makes it an offence for a man to monitor a woman's use of the internet, e-mail or other electronic communication.[46] Criminal intimidation under section 351 of the BNS, including intimidation by anonymous communication, remains available, as do sections 66E and 67 of the IT Act where images are captured or obscene material is transmitted.

Obscenity and child sexual exploitation material form a distinct sub-cluster. Electronic obscenity is punishable under sections 67 and 67A of the IT Act, while sections 294 to 296 of the BNS reproduce the old IPC provisions on obscene material.[47] Section 67B of the IT Act and sections 13 to 15 of the Protection of Children from Sexual Offences Act, 2012 (POCSO Act) govern material involving minors.[48] In *Just Rights for Children Alliance v. S. Harish*, the Supreme Court held that viewing or storing such material

---

[41]Maneela, *supra* note 33, at 575.
[42]SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra, CS (OS) No. 1279 of 2001 (Del. HC 2001) (India); *see* MALI, *supra* note 8, at 101.
[43]BNS § 356.
[44]Shreya Singhal v. Union of India, (2015) 5 SCC 1 (India).
[45]PANDEY, *supra* note 12, ¶ 7.55; BAJPAI, *supra* note 8, at 138–39.
[46]BNS § 78(1)(ii).
[47]IT Act §§ 67, 67A; BNS §§ 294–296.
[48]IT Act § 67B; The Protection of Children from Sexual Offences Act, 2012, §§ 13–15, No. 32, Acts of Parliament, 2012 (India).

amounts to "constructive possession" punishable under section 15 of the POCSO Act, and recommended that Parliament replace the term "child pornography" with "child sexual exploitative and abuse material."[49] The relationship between the IT Act and the general penal code in this field is examined in Part V.

D. Cyber Terrorism

Cyber terrorism is the use of disruptive action in cyberspace to advance political, religious or ideological objectives, including attacks on communications, transport and energy infrastructure.[50] An often-cited early instance is the 1998 campaign in which the Liberation Tigers of Tamil Eelam flooded Sri Lankan embassies with around 800 e-mails a day for two weeks.[51]

Indian infrastructure has also been affected. A disruption at Terminal 3 of Delhi's Indira Gandhi International Airport in 2013, attributed by some reports to malicious code affecting the common-use passenger processing system, illustrated the vulnerability of aviation systems.[52] The 2008 Mumbai attacks show a related phenomenon: the attackers relied on satellite imagery, GPS and internet telephony for planning and coordination.[53] That is better described as cyber-enabled terrorism than as cyber terrorism in the strict sense, but it shows how closely the two are now linked.

The IT Act as enacted contained no provision on cyber terrorism. Section 66F, inserted in 2008, punishes cyber terrorism with imprisonment that may extend to life.[54] The BNS now also defines a "terrorist act" in section 113, drawing on the Unlawful Activities (Prevention) Act, 1967, which creates a parallel route for prosecution.[55]

---

[49]Just Rts. for Child. All. v. S. Harish, 2024 INSC 716 (India).
[50]Deb, *supra* note 9, at 109.
[51]N. Veerasamy, *A High-Level Conceptual Framework of Cyber-Terrorism*, 8 J. INFO. WARFARE 43, 55 (2009).
[52]Shiv Raman & Nidhi Sharma, *Cyber Terrorism in India: A Physical Reality or Virtual Myth*, 5 INDIAN J.L. & HUM. BEHAV. (2019).
[53]*Id.*
[54]IT Act § 66F.
[55]BNS § 113.

E. Intellectual Property and Commerce-Related Offences

Software piracy is the unauthorised copying, distribution or use of software, including the installation of single-user licences on multiple machines.[56] In *Autodesk, Inc. v. Prashant Deshmukh*, the Delhi High Court expressed concern that unchecked piracy would deter investment in software development, granted a permanent injunction and awarded punitive damages.[57] Section 63B of the Copyright Act, 1957 punishes the knowing use of an infringing copy of a computer program, and sections 43(b) and 66 of the IT Act may also apply.[58]

Cyber squatting is the registration of a domain name corresponding to another's trademark in bad faith, usually to sell it back at an inflated price.[59] Indicators of bad faith include the use of false registration details, the absence of any legitimate connection between the registrant and the name, and an offer to sell at a price far above cost.[60] Neither the IT Act nor the BNS criminalises cyber squatting. Relief lies in passing off, under the Trade Marks Act, 1999, and through the .IN Domain Name Dispute Resolution Policy, and the courts have filled the gap as discussed in Part V.

Online sale of illegal articles covers narcotics, firearms, wildlife products, counterfeit currency and other contraband offered through websites, auction platforms and messaging services. It is governed by the relevant special statutes, including section 8 of the Narcotic Drugs and Psychotropic Substances Act, 1985, section 7 of the Arms Act, 1959, section 9B of the Explosives Act, 1884 and the Wild Life (Protection) Act, 1972.[61] The *Baazee.com* litigation, discussed in Part V, arose from the listing of an obscene video clip for sale on an auction website and became the foundation of Indian intermediary-liability doctrine.

---

[56] MALI, *supra* note 8, at 103.
[57] Autodesk, Inc. v. Prashant Deshmukh, (2011) 183 DLT 411 (Del. HC) (India).
[58] The Copyright Act, 1957, §§ 63, 63B, No. 14, Acts of Parliament, 1957 (India).
[59] Dipak Rao & Ravi Singhania, *Government Struggles to Keep Up with Cyber-Crime*, MANAGING INTELL. PROP. 115 (2008).
[60] PANDEY, *supra* note 12, ¶ 7.56.
[61] The Narcotic Drugs and Psychotropic Substances Act, 1985, § 8, No. 61, Acts of Parliament, 1985 (India); The Arms Act, 1959, § 7, No. 54, Acts of Parliament, 1959 (India); The Explosives Act, 1884, § 9B, No. 4 of 1884 (India); The Wild Life (Protection) Act, 1972, No. 53, Acts of Parliament, 1972 (India).

Table 1: Forms of cyber crime and their governing provisions

Cluster / form	IT Act, 2000	IPC, 1860 (repealed)	BNS, 2023 and other law
A. Systems offences			
Hacking	§§ 43(a), 66	—	—
Virus / worm	§§ 43(c), 43(e), 66	—	—
Denial of service	§§ 43(f), 66; § 66F (critical systems)	—	—
Web jacking	§§ 43, 66; § 65 (source code)	—	—
Data diddling / salami attack	§§ 43(d), 43(i), 65, 66	§ 409	§ 316(5)
Internet time theft	§§ 43(h), 66	—	—
Data theft / spyware	§§ 43(b), 66, 66E, 72, 72A	§ 379	§ 303; DPDP Act penalties
B. Fraud and deception			
Phishing	§§ 66C, 66D	§§ 419, 420	§§ 318(4), 319
Internet fraud	§§ 43, 66, 66D	§§ 415–420	§ 318; § 111 (syndicates)

Cluster / form	**IT Act, 2000**	**IPC, 1860 (repealed)**	**BNS, 2023 and other law**
Identity theft	§ 66C	§ 419	§ 319
E-mail spoofing	§ 66D	§§ 417, 419	§§ 318(2), 319
E-mail bombing	§§ 43(e), 66	—	—
Digital forgery	§§ 66C, 66D (credential misuse)	§§ 464, 465, 468, 469, 471	§§ 2(8), 335, 336, 340
C. Content offences			
Cyber defamation	§ 66A (struck down, 2015)	§§ 499, 500	§ 356
Cyber stalking	§§ 66E, 67	§§ 354D, 503, 506, 507	§§ 78, 351
Obscene material	§§ 67, 67A	§§ 292–294	§§ 294–296
Child sexual exploitation material	§ 67B	§§ 292, 293	§§ 294, 295; POCSO Act §§ 13–15
D. Cyber terrorism	§ 66F	—	§ 113; UAPA
E. IP and commerce			
Software piracy	§§ 43(b), 66	—	Copyright Act §§ 63, 63B

Cluster / form	IT Act, 2000	IPC, 1860 (repealed)	BNS, 2023 and other law
Cyber squatting	No offence	No offence	Civil: passing off; Trade Marks Act; .IN dispute policy
Online sale of illegal articles	§§ 67, 67B (content)	§ 489A (counterfeit currency)	§ 178; NDPS Act § 8; Arms Act § 7; Explosives Act § 9B; WLPA

Note: "—" indicates that the statute contains no specific provision; general provisions may still apply. BNS references are to the provision corresponding to the IPC section listed. Source: compiled by the author.

VI. THE STATUTORY ARCHITECTURE

A. Genesis and Structure of the Information Technology Act, 2000

India was among the first dozen countries to enact a dedicated cyber law.[62] The IT Act grew out of the UNCITRAL Model Law on Electronic Commerce of 1996, which the General Assembly commended to member states so that the law governing electronic communication would be uniform with that governing paper-based methods.[63] The rising use of electronic contracting, the reluctance of businesses to transact electronically without legal certainty, and the expectation that international trade bodies would move to electronic processes all supported legislation.[64]

As enacted, the IT Act comprised 94 sections in thirteen chapters and four schedules. Its opening provisions, largely modelled on the UNCITRAL text, gave legal

[62]KARNIKA SETH, CYBER LAWS IN THE INFORMATION TECHNOLOGY AGE 251 (2009).
[63]U.N. COMM'N ON INT'L TRADE L., UNCITRAL MODEL LAW ON ELECTRONIC COMMERCE WITH GUIDE TO ENACTMENT 1996, U.N. Sales No. E.99.V.4 (1999); G.A. Res. 51/162 (Dec. 16, 1996).
[64]JYOTI RATTAN, CYBER LAWS 39–40 (2011).

recognition to electronic records and digital signatures. It then set up a licensing regime for certifying authorities, a civil penalty and compensation regime in sections 43 to 45 administered by adjudicating officers, and criminal offences in sections 65 to 74.[65] The four schedules amended the IPC, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 so that they would accommodate electronic records.

B. The 2008 Amendments

Because the IT Act was designed primarily to facilitate electronic commerce, its criminal provisions soon proved inadequate. The Information Technology (Amendment) Act, 2008 transformed it into a broader cyber-crime statute.[66] The amendment removed the ₹1 crore ceiling on compensation under section 43; rewrote section 66 to require dishonest or fraudulent intent; inserted sections 66A to 66F (the last on cyber terrorism) and sections 67A to 67C; redefined "intermediary" and introduced the conditional safe harbour in section 79; empowered the Central Government to block access to information under section 69A and to monitor traffic data under section 69B; created an offence of disclosing information in breach of lawful contract in section 72A; and lowered the rank of officers competent to investigate to Inspector.[67] Table 2 summarises the IT Act offences not discussed in Part III.

Table 2: Further offences under the IT Act, 2000

Section	Offence	Gist
66B	Dishonestly receiving stolen computer resource or communication device	Receiving or retaining a stolen device or resource, knowing or believing it to be stolen.

[65] IT Act §§ 43–47, 65–74; RATTAN, *supra* note 64, at 40.
[66] The Information Technology (Amendment) Act, 2008, No. 10, Acts of Parliament, 2009 (India).
[67] *Id.*; *see* IT Act §§ 66A–66F, 67A–67C, 69A, 69B, 72A, 78, 79.

Section	Offence	Gist
66E	Violation of privacy	Intentionally capturing, publishing or transmitting images of a person's private area without consent.
71	Misrepresentation	Obtaining a licence or electronic signature certificate by misrepresenting or suppressing a material fact.
72	Breach of confidentiality and privacy	Disclosure, without consent, of material accessed in exercise of powers under the Act.
72A	Disclosure in breach of lawful contract	Disclosure of personal information obtained under a contract, with intent to cause wrongful loss or gain.
73	Publishing false electronic signature certificate	Publishing or making available a certificate known not to be genuine.
74	Publication for fraudulent purpose	Creating or publishing an electronic signature certificate for a fraudulent or unlawful purpose.

Source: IT Act §§ 66B, 66E, 71–74; compiled by the author.

Two later developments altered the institutional landscape. The Cyber Appellate Tribunal established under section 48 was merged into the Telecom Disputes Settlement and Appellate Tribunal by the Finance Act, 2017,[68] and the Indian

[68]The Finance Act, 2017, No. 7, Acts of Parliament, 2017, pt. XIV (India).

Computer Emergency Response Team (CERT-In) issued directions under section 70B(6) in 2022 that require service providers and other entities to report specified cyber incidents within six hours.[69] A private member's Bill, the Information Technology (Amendment) Bill, 2018, introduced in the Rajya Sabha by Narayan Lal Panchariya on 3 August 2018, would have criminalised content repugnant to "cultural ethos" and online games inducing self-harm, a response to the "Blue Whale" challenge, but, lacking government sponsorship, it was not enacted.[70]

C. Intermediary Regulation: The 2021 Rules and the 2026 Amendment

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 shifted the regulatory focus from offenders to platforms.[71] As made in 2021, they required intermediaries to remove content within thirty-six hours of a court order or government notification, to remove non-consensual intimate imagery within twenty-four hours of a complaint, to appoint grievance officers who must acknowledge complaints within twenty-four hours and resolve them within fifteen days, to publish periodic compliance reports, and to comply with emergency blocking. Significant social media intermediaries carry additional obligations.

The February 2026 amendment, in force from 20 February 2026, shortened these windows to three hours for court or government directions, two hours for non-consensual intimate imagery and seven days for grievance resolution. It also introduced a definition of "synthetically generated information," covering audio, visual or audio-visual content that is artificially created or altered so as to appear authentic, and requires such content to carry a prominent label and provenance

---

[69]Indian Computer Emergency Response Team, Directions Under Sub-section (6) of Section 70B of the Information Technology Act, 2000, No. 20(3)/2022-CERT-In (Apr. 28, 2022) (India).
[70]The Information Technology (Amendment) Bill, 2018, Bill No. [●] of 2018 (introduced in the Rajya Sabha by Shri Narayan Lal Panchariya on Aug. 3, 2018) (India) (private member's Bill proposing new sections 67BA and 67BB); ACCESS NOW, DIGITAL RIGHTS IN INDIA'S PARLIAMENT (Aug. 2019), https://www.accessnow.org/wp-content/uploads/2019/08/Access-Now-Digital-Rights-in-Indias-Parliament-August-2019.pdf; *see also* Andrew Rossow, *Cyberbullying Taken to a Whole New Level: Enter the Blue Whale Challenge*, FORBES (Feb. 28, 2018), https://www.forbes.com/sites/andrewrossow/2018/02/28/cyberbullying-taken-to-a-whole-new-level-enter-the-blue-whale-challenge/ (background on the Blue Whale challenge).
[71]Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E) (Feb. 25, 2021) (India) [hereinafter IT Rules, 2021].

metadata.[72] This is the first Indian legal instrument to address deepfakes in terms, and it bears directly on impersonation fraud, non-consensual imagery and election misinformation.

D. The New Criminal Codes and the DPDP Act

The BNS does not create a separate chapter on cyber crime, but it modernises the general penal law in several ways that matter. It treats electronic records as documents throughout; it consolidates the cheating offences into sections 318 and 319; it brings "cyber-crimes" committed by syndicates within the organised-crime offence in section 111, with minimum sentences of five years for members; and it adds a terrorism offence in section 113.[73] The BNSS permits the electronic registration of FIRs, requires forensic investigation for offences punishable with seven years or more, and provides for audio-video recording of searches.[74] The BSA classifies electronic records as documentary evidence and, in section 63, carries forward the certificate requirement of former section 65B of the Evidence Act, now in a prescribed form signed by both the person in charge of the device and an expert.[75]

The DPDP Act adds a regulatory layer. It imposes duties on data fiduciaries, including a duty to take reasonable security safeguards and to notify personal data breaches, to be enforced through monetary penalties imposed by the Data Protection Board of India. The Board was established in November 2025, but these duties and the penalty provisions take effect only from 13 May 2027.[76] The Act is not a criminal statute, but it creates incentives for prevention that the IT Act's after-the-fact offences do not, and those incentives will operate only prospectively.

---

[72]IT Rules, 2021, rr. 3(1)(d), 3(2)(a)(i), 3(2)(b), as amended by G.S.R. 120(E), *supra* note 7 (in force Feb. 20, 2026); *Govt Tightens Rules on AI-Generated Content, Mandates Labels and Faster Takedowns*, BUSINESS TODAY (Feb. 10, 2026), https://www.businesstoday.in/technology/story/govt-tightens-rules-on-ai-generated-content-mandates-labels-and-faster-takedowns-515505-2026-02-10.
[73]BNS §§ 2(8), 111, 113, 318, 319.
[74]BNSS §§ 105, 173, 176(3).
[75]BSA §§ 2(1)(d), 61, 63.
[76]DPDP Act §§ 8(5)–(6), 33 & sch.; *see supra* note 6 (commencement schedule).

E. Other Statutes

Several other statutes complete the framework. The Prevention of Money Laundering Act, 2002 defines "records" to include electronic records, which brings the proceeds of cyber fraud within its reach.[77] The Companies (Management and Administration) Rules, 2014 impose security obligations in respect of electronic records and e-voting. Online money gaming is now governed by the Promotion and Regulation of Online Gaming Act, 2025, in force from 1 May 2026, which prohibits the offering and advertising of online money games and the transfer of funds for them, punishes the offering of such games with imprisonment of up to three years and a fine of up to ₹1 crore, and provides for a central Authority on Online Gaming; its constitutional validity is under challenge before the Supreme Court.[78]

The Public Gambling Act, 1867 and state gambling laws, earlier applied to online betting, remain relevant chiefly to offline gambling. The Copyright Act, 1957, the Trade Marks Act, 1999 and the Patents Act, 1970 protect intellectual property in electronic form. Table 3 lists the provisions of the general penal code, other than those discussed in Part III, that are most often invoked in cyber cases.

Table 3: General penal provisions frequently invoked in cyber cases

Offence	IPC, 1860	BNS, 2023	Typical cyber context
Criminal conspiracy	§ 120B	§ 61(2)	Fraud syndicates; coordinated attacks

[77]The Prevention of Money-Laundering Act, 2002, § 2(1)(w), No. 15, Acts of Parliament, 2003 (India).
[78]The Promotion and Regulation of Online Gaming Act, 2025, §§ 5–9, No. 32, Acts of Parliament, 2025 (India) (in force May 1, 2026, by Notification S.O. 1994(E) (Apr. 22, 2026)); Head Digital Works Pvt. Ltd. v. Union of India, Transferred Case (C) No. [●] of 2025 (SC) (India) (challenges transferred from the High Courts of Delhi, Karnataka and Madhya Pradesh in September 2025 and pending as of Nov. 24, 2026).

Offence	IPC, 1860	BNS, 2023	Typical cyber context
Promoting enmity between groups	§ 153A	§ 196	Hate content on social media
Outraging religious feelings	§ 295A	§ 299	Inflammatory posts and videos
Printing or engraving defamatory matter	§ 501	§ 356(3)	Republication of defamatory content
Statements conducing to public mischief	§ 505	§ 353	Online rumours and misinformation
Criminal intimidation by anonymous communication	§ 507	§ 351(4)	Threats from anonymous or fake accounts
Insulting the modesty of a woman	§ 509	§ 79	Abusive messages and images

Source: IPC; BNS; compiled by the author.

VII. THE JUDICIAL RESPONSE

The courts have shaped Indian cyber law as much as Parliament has, sometimes by applying general principles to new facts and sometimes by filling statutory gaps. Six areas of judicial activity can be identified.

A. Early Prosecutions and Data Tampering

The *Sony.Sambandh.com* case is widely described as India's first cyber-crime conviction. In May 2002, a person using a stolen credit card ordered a colour television and a cordless headphone through Sony India's website for non-resident Indians, for

delivery to Arif Azim in Noida. When the cardholder disputed the transaction, the Central Bureau of Investigation traced the goods to Azim, a call-centre employee who had misused the card details. In February 2003, a Metropolitan Magistrate in New Delhi convicted him under sections 418, 419 and 420 of the IPC and released him on probation for one year.[79] It is significant that the conviction rested entirely on the general penal code rather than on the IT Act; *Suhas Katti*, discussed below, is separately described as the first conviction under section 67 of the IT Act.

Data-tampering cases followed. In *State of Maharashtra v. Rajkumar Kunda Swami*, a bank clerk who had allegedly opened fictitious accounts and manipulated credit entries in a co-operative bank's computer system was prosecuted under sections 43, 65, 66 and 73 of the IT Act and section 409 and the cheating and forgery provisions of the IPC; the loss, put at ₹81 lakh in the complaint, exceeded ₹2.27 crore on investigation. The Bombay High Court set aside the bail granted by the Magistrate, holding that he lacked jurisdiction to grant bail for an offence under section 409 punishable with imprisonment for life, but refused further police custody.[80] The case remains an early IT Act prosecution for the manipulation of bank data.

In *Syed Asifuddin v. State of Andhra Pradesh*, the Andhra Pradesh High Court held that reprogramming the electronic serial number of handsets locked to one network operator amounted to tampering with computer source code under section 65.[81] In *Firos v. State of Kerala*, the Kerala High Court upheld the notification of the FRIENDS e-governance software as a "protected system" under section 70 and the constitutional validity of that section.[82] The *Bank NSP* case, in which a management trainee used her

[79]*Red Alert, Netizens!*, DATAQUEST (Sept. 14, 2004), https://www.dqindia.com/red-alert-netizens/; *India Gets Its First Cyber Convict*, OODA LOOP (Feb. 6, 2003), https://oodaloop.com/realnews-items/2003/02/06/6425. The trial court judgment is unreported; these contemporaneous reports are the closest available record of the conviction.

[80]State of Maharashtra v. Rajkumar Kunda Swami, (2002) 104(3) Bom. L.R. 567 (Bom. HC Dec. 4, 2001) (India).

[81]Syed Asifuddin v. State of Andhra Pradesh, 2005 Cri. L.J. 4314 (A.P. HC) (India).

[82]Firos v. State of Kerala, AIR 2006 Ker. 279 (India).

employer's systems to send fabricated e-mails to her former fiancé's clients, established that a bank could be liable for e-mails sent through its systems.[83]

B. Domain Names and Phishing: Filling Legislative Gaps

The most visible judicial creativity has been in areas Parliament left untouched. In *Yahoo!, Inc. v. Akash Arora*, the Delhi High Court restrained the defendants from using "yahooindia.com" for internet services,[84] and in *Rediff Communication Ltd. v. Cyberbooth* the Bombay High Court held that a domain name is more than an internet address and is entitled to protection equal to that of a trademark.[85] The Supreme Court confirmed this approach in *Satyam Infoway Ltd. v. Sifynet Solutions (P) Ltd.*, holding that domain names are subject to the law of passing off because confusingly similar names divert users who access the wrong site.[86] As a result, cyber squatting is effectively controlled through civil remedies even though it is not a crime.

Phishing followed the same path. In *National Association of Software and Service Companies v. Ajay Sood*, the Delhi High Court observed that India had no legislation on phishing, characterised it as a misrepresentation in the course of trade amounting to passing off, and granted an injunction and damages.[87] Parliament then inserted sections 66C and 66D in 2008, which suggests that judicial innovation can prompt legislative correction.

C. Obscenity, Speech and the Special-Law Question

The obscenity cases show the courts balancing protection against expression. In *Ranjit D. Udeshi v. State of Maharashtra*, the Supreme Court upheld section 292 of the IPC as a reasonable restriction under Article 19(2) in the interests of decency and morality, and adopted the English Hicklin test, which asked whether isolated passages tended

[83] *See* Sarmah, Sarmah & Baruah, *supra* note 22, at 1636.
[84] Yahoo!, Inc. v. Akash Arora, (1999) 19 PTC 201 (Del. HC) (India).
[85] Rediff Commc'n Ltd. v. Cyberbooth, AIR 2000 Bom. 27 (India).
[86] Satyam Infoway Ltd. v. Sifynet Sols. (P) Ltd., (2004) 6 SCC 145 (India).
[87] Nat'l Ass'n of Software & Serv. Cos. v. Ajay Sood, (2005) 119 DLT 596 (Del. HC) (India).

to deprave and corrupt those open to immoral influences.[88] In *Ajay Goswami v. Union of India*, the Court accepted that restrictions on obscene content are justified but warned against reducing adult expression to what is fit for children.[89] *Suhas Katti v. State of Tamil Nadu*, in which a rejected suitor posted obscene messages about a woman in Yahoo groups, produced the first conviction under section 67 of the IT Act, together with sections 469 and 509 of the IPC, within months of the complaint.[90]

The Hicklin test adopted in *Ranjit Udeshi* no longer governs. In *Aveek Sarkar v. State of West Bengal*, the Supreme Court discarded it in favour of a "community standards" test, under which material is judged as a whole, from the point of view of an average person applying contemporary community standards, and in the light of its context and message.[91] The Court has applied that test to electronic content, holding in *Apoorva Arora v. State (Government of NCT of Delhi)* that vulgar or profane language in a web series is not, without more, obscene under sections 67 and 67A of the IT Act.[92] The same standard now governs those sections and sections 294 to 296 of the BNS, while *Ranjit Udeshi* remains authority for the validity of the obscenity offence under Article 19(2).

Sharat Babu Digumarti v. Government (NCT of Delhi) resolved an important question of statutory relationship. The Supreme Court held that where the IT Act deals specifically with obscenity in electronic form, a person cannot be prosecuted for the same conduct under section 292 of the IPC, because the special enactment prevails over the general.[93] The High Courts have since marked the limits of that rule. In *Gagan Harsh Sharma v. State of Maharashtra*, a Division Bench of the Bombay High Court read *Sharat Babu* to hold that dishonest or fraudulent acts covered by sections 43 and 66 of the IT Act displace prosecution for theft, cheating and criminal breach of trust under

---

[88]Ranjit D. Udeshi v. State of Maharashtra, AIR 1965 SC 881 (India) (applying Regina v. Hicklin, (1868) LR 3 QB 360 (Eng.)); *see* CYBER SPACE AND THE LAW: ISSUES AND CHALLENGES 198 (Ranbir Singh & Ghanshyam Singh eds., 2004).
[89]Ajay Goswami v. Union of India, (2007) 1 SCC 143 (India).
[90]Suhas Katti v. State of Tamil Nadu, C.C. No. 4680 of 2004 (Addl. Chief Metro. Magis., Egmore, Nov. 5, 2004) (India).
[91]Aveek Sarkar v. State of West Bengal, (2014) 4 SCC 257, ¶¶ 24–25 (India).
[92]Apoorva Arora v. State (Gov't of NCT of Delhi), 2024 INSC 223 (India).
[93]Sharat Babu Digumarti v. Gov't (NCT of Delhi), (2017) 2 SCC 18 (India).

the IPC.[94] On 15 April 2024, a Full Bench at Aurangabad declined to follow that view in *Awadhesh Kumar Parasnath Pathak v. State of Maharashtra*.

Relying on *State of Uttar Pradesh v. Aman Mittal*, it held that the special law excludes the IPC only where both offences share the same ingredients; because cheating requires deceit, which sections 43 and 66 do not, both statutes may be invoked, subject to the bar on double punishment.[95] No challenge to the Full Bench decision before the Supreme Court has been reported. The BNS is a later enactment that covers electronic records, and that ingredient-based test, together with the maxim *generalia specialibus non derogant*, must now be applied afresh to each overlapping pair. Part VI returns to this point.

D. Intermediary Liability

The liability of platforms has generated the most consequential case law. In *Avnish Bajaj v. State*, the managing director of Baazee.com was prosecuted after an obscene clip was listed for sale on the site; the Delhi High Court declined to quash the proceedings under section 67 of the IT Act.[96] The Supreme Court later quashed them in *Aneeta Hada v. Godfather Travels & Tours Pvt. Ltd.*, holding that a director cannot be vicariously prosecuted under section 85 of the IT Act unless the company itself is arraigned.[97] Meanwhile, Parliament had introduced the safe harbour in section 79.

Shreya Singhal then struck down section 66A and read down section 79(3)(b), holding that an intermediary must remove content only on receiving actual knowledge through a court order or government notification relating to the grounds in Article 19(2).[98] Section 66A nonetheless continued to be invoked, and in 2022 the Supreme Court directed that no prosecution may proceed under it.[99] More recently, in *X Corp.*

---

[94]Gagan Harsh Sharma v. State of Maharashtra, 2019 Cri. L.J. 1398 (Bom. HC) (India).
[95]Awadhesh Kumar Parasnath Pathak v. State of Maharashtra, 2024 SCC OnLine Bom 1074 (Bom. HC Apr. 15, 2024) (India) (Full Bench, Criminal Application No. 2562 of 2019); State of Uttar Pradesh v. Aman Mittal, (2019) 19 SCC 740 (India).
[96]Avnish Bajaj v. State, (2008) 105 DRJ 721 (Del. HC) (India).
[97]Aneeta Hada v. Godfather Travels & Tours (P) Ltd., (2012) 5 SCC 661 (India) (deciding Avnish Bajaj's appeal together with the lead appeal).
[98]Shreya Singhal, *supra* note 44.
[99]People's Union for C.L. v. Union of India, Misc. Application No. 901 of 2021 in Writ Petition (Crl.) No. 199 of 2013 (SC Oct. 12, 2022) (India).

v. Union of India, the Karnataka High Court upheld the Sahyog portal, through which government agencies send takedown notices under section 79(3)(b) read with the 2021 Rules, holding that section 79(3)(b) operates independently of the blocking procedure in section 69A.[100]

A Division Bench admitted X Corp's writ appeal in March 2026, but on 22 July 2026 the Supreme Court stayed that appeal and connected challenges in the Karnataka and Bombay High Courts on transfer petitions filed by the Union; as of November 2026, the transfer petitions remained pending.[101] Taken together, the decisions show an unresolved tension between speed of takedown, which is valuable against fraud and non-consensual imagery, and the procedural safeguards that *Shreya Singhal* insisted on.

E. Privacy and Surveillance

The recognition of privacy as a fundamental right in *K.S. Puttaswamy v. Union of India* changed the constitutional backdrop against which interception and data-extraction powers must be assessed.[102] The Pegasus allegations tested that framework. West Bengal appointed a commission of inquiry headed by Justice Madan B. Lokur,[103] but the decisive step came when the Supreme Court in *Manohar Lal Sharma v. Union of India* appointed a technical committee supervised by Justice R.V. Raveendran, holding that a bare invocation of national security cannot exclude judicial review.[104]

---

[100]X Corp. v. Union of India, Writ Petition No. 7405 of 2025 (Kar. HC Sept. 24, 2025) (India).
[101]Union of India v. X Corp., Transfer Petition (C) No. [●] of 2026 (SC July 22, 2026) (India) (order issuing notice and staying the High Court proceedings); *Supreme Court Stays HC Proceedings in Pleas of X Corp, Kunal Kamra & Others Against Sahyog Portal, Content Blocking Powers*, LIVELAW (Aug. 2026), https://www.livelaw.in/top-stories/supreme-court-stays-hc-proceedings-in-pleas-of-x-corp-kunal-kamra-others-against-sahyog-portal-content-blocking-powers-544774; *Karnataka High Court Issues Notice to Centre on X Corp's Appeal Against Sahyog Portal*, LIVELAW (Mar. 10, 2026), https://www.livelaw.in/high-court/karnataka-high-court/karnataka-high-court-x-corp-challenges-it-act-framework-525827.
[102]K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 (India).
[103]Aaratrika Bhaumik, *West Bengal Govt Constitutes Panel Headed by Justice Madan Lokur to Probe Pegasus Scandal*, LIVELAW (July 26, 2021), https://www.livelaw.in/news-updates/west-bengal-government-pegasus-scandal-justice-madan-lokur-justic-jyotirmay-bhattacharya-178154.
[104]Manohar Lal Sharma v. Union of India, 2021 SCC OnLine SC 985 (India).

In August 2022 the Court recorded that malware had been found on five of the twenty-nine devices examined, but that it could not be conclusively identified as Pegasus, and that the Union had not cooperated with the committee.[105] The episode shows both the reach and the limits of judicial oversight where the state itself is the suspected intruder.

F. Electronic Evidence and Investigative Direction

Cyber prosecutions often fail on proof. In *Anvar P.V. v. P.K. Basheer*, the Supreme Court held that a certificate under section 65B (4) of the Evidence Act is mandatory for secondary electronic evidence, and *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* confirmed that position.[106] Section 63 of the BSA preserves and tightens the requirement, so these decisions remain the governing framework.

Most recently, in the digital arrest proceedings, the Supreme Court has gone beyond adjudication: it has designated the CBI as the primary investigating agency, authorised inquiry into the role of bank officials in opening mule accounts, and issued directions on prevention, compensation and grievance redressal.[107] This is judicial activism of a new kind, which addresses the institutional weaknesses of enforcement rather than gaps in doctrine.

VIII. CRITICAL APPRAISAL

Five structural weaknesses emerge from this survey:

First, fragmentation and overlap. Cyber offences are spread across the IT Act, the BNS, the POCSO Act, intellectual property statutes and sectoral laws, with no definition of "cyber crime" and no consolidated schedule. Most conduct can be charged under two or more statutes with different penalties, bail consequences and limitation periods.

---

[105] *Pegasus: Malware Found on Five Phones but Evidence Is Inconclusive, Says SC-Appointed Panel*, SCROLL.IN (Aug. 25, 2022), https://scroll.in/latest/1031257.

[106] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473 (India); Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1 (India).

[107] *In re* Victims of Digital Arrest, *supra* note 4; *Digital Arrest Scams: Supreme Court Issues Directions for Prevention, Compensation & Grievance Redressal*, LIVELAW (Aug. 4, 2026), https://www.livelaw.in/top-stories/digital-arrest-scams-supreme-court-issues-directions-for-prevention-compensation-greivance-redressal-544292.

Phishing, for example, may attract section 66D of the IT Act (up to three years) and section 318(4) of the BNS (up to seven years). *Sharat Babu* resolved one such overlap in favour of the special law,[108] and the Bombay High Court's Full Bench has since confined that rule to offences with identical ingredients.[109] On that test, section 66D does not displace section 318(4), which additionally requires dishonest inducement to deliver property, but it arguably displaces section 319, whose ingredients it reproduces with the added element of a computer resource. The test still leaves open whether a later general code alters the special-law presumption, and it binds only one High Court. Without legislative guidance, the choice between statutes rests with individual investigating officers, which produces inconsistency and invites forum-driven charging.

Secondly, substantive gaps. Cyber squatting remains outside penal law; salami attacks and data diddling are prosecuted under general provisions that do not reflect their aggregated harm; and e-mail bombing and DoS attacks are treated under section 66, which does not distinguish between a nuisance and an attack on critical infrastructure unless the high threshold of section 66F is met. Section 78 of the BNS remains gender-specific, so a man cyber-stalked by another person, or a woman stalked by a woman, falls outside it.[110] The term "cyber-crimes" in section 111 is undefined, which risks both over-inclusion and challenge.[111] Despite the 2026 amendment, the treatment of synthetic media remains regulatory rather than penal, and it is not yet clear how impersonation through deepfakes maps onto sections 66C, 66D and 319.

Thirdly, enforcement capacity. Rising registrations do not translate into resolution. In 2023 Karnataka recorded 21,889 cases but a charge-sheeting rate of only 18.1 per cent, and Telangana recorded a rate of 20.9 per cent.[112] At the end of 2024, approximately

---

[108]Sharat Babu Digumarti, *supra* note 93.
[109]Awadhesh Kumar Parasnath Pathak, *supra* note 95; *see* BNS § 9; The General Clauses Act, 1897, § 26, No. 10, Acts of Parliament, 1897 (India).
[110]BNS § 78(1).
[111]BNS § 111(1).
[112]NAT'L CRIME RECORDS BUREAU, MINISTRY OF HOME AFFS., CRIME IN INDIA 2023, *supra* note 2, tbl. 9A.1; *see also B'luru Cybercrime Tally More than Top 10 Cities' Total*, DECCAN HERALD (Oct. 2025), https://www.deccanherald.com/india/karnataka/bengaluru/b-luru-cybercrime-tally-more-than-top-10-cities-total-3748817; *Telangana Tops India in Cybercrime*, DECCAN CHRONICLE (Oct. 2025),

1.2 lakh cyber-crime cases remained pending investigation.[113] Early cases such as *Col. Bajwa* reportedly exposed a lack of technical expertise among investigators,[114] and that problem persists at scale despite the Indian Cyber Crime Coordination Centre and the national reporting portal. The adjudication machinery under the IT Act has also weakened: adjudicating officers are senior state civil servants, and the merger of the Cyber Appellate Tribunal into a telecom tribunal has removed a specialist appellate forum.

Fourthly, the cross-border dimension. Section 75 gives the IT Act extraterritorial reach where a computer system located in India is involved,[115] but jurisdiction is of little use without evidence and extradition. Much cyber fraud targeting Indians is conducted from abroad, and mutual legal assistance processes are slow relative to the speed with which funds move. India's signature of the UN Convention against Cybercrime is a significant step, but it does not create domestic obligations until ratification, and the Convention's provisions on cross-border preservation and production of electronic evidence will need implementing legislation.[116]

Fifthly, victim redress. Indian cyber law remains oriented towards punishing offenders rather than restoring victims. The compensation route under section 43, which produced the award in *Umashankar*, is little used and depends on adjudicating officers who are senior state civil servants with many other responsibilities. Until recently, banking customers relied on the Reserve Bank of India's 2017 limited-liability framework, which covered only unauthorised transactions and did not reach payments that the victim was manipulated into authorising. The Reserve Bank's amendment directions of June 2026, which apply to transactions from 1 January 2027, extend protection to "fraudulent" transactions, including payments that a customer

---

https://www.deccanchronicle.com/southern-states/telangana/telangana-tops-india-in-cybercrime-1907213. Karnataka's charge-sheeting rate rose only to 22.1 per cent in 2024. CRIME IN INDIA 2024, *supra* note 3, tbl. 9A.1.

[113]CRIME IN INDIA 2024, *supra* note 3, ch. 9A (Police Disposal of Cyber Crime Cases); *see also Cybercrime Cases Rise 18 Percent Across India, NCRB Report Flags Fraud as Biggest Motive*, THE420.IN (May 2026), https://the420.in/?p=113290.

[114]PANDEY, *supra* note 12, ¶ 4.3; *see supra* note 26 (on the sources for the case).

[115]IT Act § 75.

[116]G.A. Res. 79/243, *supra* note 14.

approves under coercion or duress, place the burden of proof on the bank, and provide a one-time compensation of 85 per cent of the net loss, capped at ₹25,000, for losses of up to ₹50,000.[117] The gap narrows but does not close. Payments that a deceived customer makes without coercion, typical of investment scams, fall outside the new definition; larger losses still turn on findings of bank negligence or customer fault; and the protection rests on regulatory directions rather than statute. The Supreme Court's 2026 directions on compensation address part of this gap,[118] but a lasting solution requires legislation.

A. A Comparative Note

Comparative experience suggests that these weaknesses are not inevitable. The United Kingdom's Computer Misuse Act, 1990 organises cyber-dependent offences into a short, graded sequence running from unauthorised access, to access with intent to commit further offences, to unauthorised acts impairing a computer and, at the top, acts causing or creating a risk of serious damage to human welfare, the economy or national security.[119] The United States' Computer Fraud and Abuse Act similarly grades penalties by harm, loss and the nature of the protected computer.[120] India's section 66, by contrast, treats nearly all section 43 conduct as a single offence carrying up to three years, with section 66F available only at the extreme.

Singapore's Online Criminal Harms Act, 2023 offers a different lesson: it equips authorities to issue directions to platforms against online activity facilitating scams, with defined procedures and appeal routes,[121] which is the kind of structured framework that the Sahyog litigation shows India currently lacks. The Budapest

---

[117]Reserve Bank of India (Commercial Banks - Responsible Business Conduct) Third Amendment Directions, 2026, RBI/2026-27/167, DOR.MCS.REC.No.130/01-01-032/2026-27, ¶¶ 4(15A), 76A–76V (June 24, 2026) (India) (applicable to transactions on or after Jan. 1, 2027, and replacing the limited-liability instructions first issued as RBI/2017-18/15 (July 6, 2017)); Reserve Bank of India, Press Release, *RBI Issues Amendment Directions on 'Review of Framework of Limiting Customer Liability in Digital Transactions'* (June 24, 2026), https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=63011.

[118]*Digital Arrest Scams: Supreme Court Issues Directions*, *supra* note 107.

[119]Computer Misuse Act 1990, c. 18, §§ 1–3ZA (UK).

[120]18 U.S.C. § 1030 (2018).

[121]Online Criminal Harms Act 2023 (Sing.).

Convention, finally, demonstrates the value of a common vocabulary of offences and procedural powers such as expedited preservation of stored data, which Indian law grants only partially and in scattered form.[122] None of these models can be transplanted wholesale, but together they point towards grading by harm, a consolidated offence list and procedural powers designed for volatile electronic evidence.

IX. SUGGESTIONS AND RECOMMENDATIONS

Six reforms follow from this analysis:

First, Parliament should enact a statutory definition of "cyber crime" and a consolidated schedule that identifies, for each recognised form, the primary offence and the provisions to be applied alongside it. The long-proposed Digital India Act, which is intended to replace the IT Act, is the natural vehicle.[123] Pending that, the Union should issue charging guidelines to police and prosecutors.

Secondly, Parliament should settle the relationship between the IT Act and the BNS expressly. The ingredient-based test of the Bombay High Court's Full Bench resolves overlaps only offence by offence, binds no other High Court, and leaves open how a later general code interacts with an earlier special statute. A saving clause that specifies, for each overlapping pair, whether the offences are alternative or cumulative would remove that residual uncertainty more reliably than case-by-case application of the special-law maxim after *Sharat Babu*.

Thirdly, specific gaps should be closed: section 78 of the BNS should be made gender-neutral; bad-faith domain registration should be made an offence where it is linked to fraud or impersonation; DoS and malware offences should be graded by harm; and the creation or distribution of deceptive synthetic media for fraud or sexual

[122]Convention on Cybercrime, *supra* note 13, arts. 16–17.
[123]*Explained: How Digital India Act Will Replace Old IT Regime to Tame Big Tech, Safeguard Users*, MORUNG EXPRESS (Mar. 10, 2023), https://morungexpress.com/explained-how-digital-india-act-will-replace-old-it-regime-to-tame-big-tech-safeguard-users.

exploitation should carry a specific penal provision to complement the labelling regime of 2026.

Fourthly, investment in enforcement capacity should match legislative ambition. This means dedicated cyber-crime units with forensic laboratories in every district, a revived specialist appellate tribunal, standard operating procedures for the BSA section 63 certificate, and real-time coordination between banks, telecom providers and police for freezing funds, building on the Supreme Court's directions in the digital arrest proceedings.

Fifthly, Parliament should place the Reserve Bank's 2026 customer-protection framework on a statutory footing and extend it to what that framework leaves uncovered. Victims of authorised-push-payment frauds induced by deception should have a statutory route to restitution, including a duty on banks and payment providers to act on fraud alerts in real time, a presumption of shared liability where mule accounts were opened without adequate verification, and a fast-track compensation mechanism above the regulatory ceiling that does not depend on the conviction of the offender.

Finally, India should move promptly to ratify the UN Convention against Cybercrime with reservations that protect constitutional guarantees, and should negotiate bilateral agreements for direct production of electronic evidence from service providers abroad, with *Puttaswamy*-compliant safeguards.

X. CONCLUSION

India's legal response to cyber crime has been incremental and reactive, driven partly by legislation and partly by judicial creativity. The IT Act, conceived as an electronic-commerce statute, became a cyber-crime statute through the 2008 amendments. The general penal law, now recodified in the BNS, has absorbed much cyber-enabled crime. The courts have filled gaps in the treatment of domain names and phishing, defined the limits of intermediary liability, and, most recently, begun to direct investigation itself. The typology developed here shows that almost every prevalent form of cyber crime can be addressed somewhere in Indian law.

Breadth, however, is not the same as coherence. The framework is fragmented across overlapping statutes, rests on undefined central terms, leaves certain harmful practices outside penal law, and depends on an enforcement apparatus that resolves only a fraction of the cases it registers. With registrations now above one lakh a year and fraud dominant, these weaknesses are no longer marginal. The transition to the new criminal codes, the phased commencement of the DPDP Act and India's signature of the UN Convention together create a rare opportunity for consolidated reform. Whether that opportunity is used will decide whether Indian cyber law moves from a patchwork of responses to a coherent regime capable of matching the scale and sophistication of the crime it confronts.

XI. REFERENCES

A. Statutes and Subordinate Legislation

1. 18 U.S.C. § 1030 (2018) (Computer Fraud and Abuse Act).
2. The Arms Act, 1959, No. 54, Acts of Parliament, 1959 (India).
3. The Bharatiya Nagarik Suraksha Sanhita, 2023, No. 46, Acts of Parliament, 2023 (India).
4. The Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023 (India).
5. The Bharatiya Sakshya Adhiniyam, 2023, No. 47, Acts of Parliament, 2023 (India).
6. Computer Misuse Act 1990, c. 18 (UK).
7. Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185.
8. The Copyright Act, 1957, No. 14, Acts of Parliament, 1957 (India).
9. The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
10. Digital Personal Data Protection Rules, 2025, G.S.R. 846(E) (Nov. 13, 2025) (India).
11. The Explosives Act, 1884, No. 4 of 1884 (India).

12. The Finance Act, 2017, No. 7, Acts of Parliament, 2017 (India).
13. Online Criminal Harms Act 2023 (Sing.).
14. The Prevention of Money-Laundering Act, 2002, No. 15, Acts of Parliament, 2003 (India).
15. The Promotion and Regulation of Online Gaming Act, 2025, No. 32, Acts of Parliament, 2025 (India).
16. The Protection of Children from Sexual Offences Act, 2012, No. 32, Acts of Parliament, 2012 (India).
17. Reserve Bank of India, Customer Protection: Limiting Liability of Customers in Unauthorised Electronic Banking Transactions, RBI/2017-18/15, DBR.No.Leg.BC.78/09.07.005/2017-18 (July 6, 2017) (India).
18. Reserve Bank of India (Commercial Banks - Responsible Business Conduct) Third Amendment Directions, 2026, RBI/2026-27/167, DOR.MCS.REC.No.130/01-01-032/2026-27 (June 24, 2026) (India).
19. The Wild Life (Protection) Act, 1972, No. 53, Acts of Parliament, 1972 (India).

B. Books

1. FAROOQ AHMAD, CYBER LAW IN INDIA (LAW ON INTERNET) (3d ed. 2008).
2. G.S. BAJPAI, ON CYBER CRIME & CYBER LAW (2011).
3. CYBER SPACE AND THE LAW: ISSUES AND CHALLENGES (Ranbir Singh & Ghanshyam Singh eds., 2004).
4. PRASHANT MALI, CYBER LAW & CYBER CRIMES (2012).
5. ASHISH PANDEY, CYBER CRIMES: DETECTION & PREVENTION (2006).
6. JYOTI RATTAN, CYBER LAWS (2011).
7. KARNIKA SETH, CYBER LAWS IN THE INFORMATION TECHNOLOGY AGE (2009).
8. S.K. VERMA & RAMAN MITTAL, LEGAL DIMENSIONS OF CYBER SPACE (2004).

C. Articles

1. Abhijeet Deb, *Cyber Crime and Judicial Response in India*, 3 INDIAN J.L. & JUST. 106 (2012).
2. V.M. Eshwar & Aswathy Rajan, *A Critical Analysis on Judicial Activism in Relation to Cyber Law: An Indian Perspective*, 119 INT'L J. PURE & APPLIED MATHEMATICS 1489 (2018).
3. Maneela, *Cyber Crimes: The Indian Legal Scenario*, 11 U.S.-CHINA L. REV. 570 (2014).
4. Animesh Sarmah, Roshmi Sarmah & Amlan Jyoti Baruah, *A Brief Study on Cyber Crime and Cyber Laws of India*, 4 INT'L RSCH. J. ENG'G & TECH. 1633 (2017).
5. N. Veerasamy, *A High-Level Conceptual Framework of Cyber-Terrorism*, 8 J. INFO. WARFARE 43 (2009).

D. Online Sources

1. *22-Year-Old Student Held for Hacking GTU Portal, Stealing and Leaking Data*, INDIAN EXPRESS (Aug. 20, 2020), https://indianexpress.com/article/india/22-year-old-student-held-for-hacking-gtu-portal-stealing-and-leaking-data-6561971/.
2. *Bengaluru Records 17,561 Cybercrime Cases in 2024, Highest Among Metro Cities Again*, NEWS MINUTE (May 2026), https://www.thenewsminute.com/karnataka/bengaluru-records-17561-cybercrime-cases-in-2024-highest-among-metro-cities-again.
3. Aaratrika Bhaumik, *West Bengal Govt Constitutes Panel Headed by Justice Madan Lokur to Probe Pegasus Scandal*, LIVELAW (July 26, 2021), https://www.livelaw.in/news-updates/west-bengal-government-pegasus-scandal-justice-madan-lokur-justic-jyotirmay-bhattacharya-178154.

4. *B'luru Cybercrime Tally More than Top 10 Cities' Total*, DECCAN HERALD (Oct. 2025), https://www.deccanherald.com/india/karnataka/bengaluru/b-luru-cybercrime-tally-more-than-top-10-cities-total-3748817.

5. *The Curious Case of Ken Haywood*, INDIAN EXPRESS (Aug. 14, 2008), http://archive.indianexpress.com/news/the-curious-case-of-ken-haywood/348646/.

6. *Cybercrime Cases Rise 18 Percent Across India, NCRB Report Flags Fraud as Biggest Motive*, THE420.IN (May 2026), https://the420.in/?p=113290.

7. *Cybercrime Soars by 31% in India, Karnataka Tops with 21,889 Cases*, NEWS MINUTE (Sept. 30, 2025), https://www.thenewsminute.com/news/cybercrime-soars-by-31-in-india-karnataka-tops-with-21889-cases.

8. *Govt Tightens Rules on AI-Generated Content, Mandates Labels and Faster Takedowns*, BUSINESS TODAY (Feb. 10, 2026), https://www.businesstoday.in/technology/story/govt-tightens-rules-on-ai-generated-content-mandates-labels-and-faster-takedowns-515505-2026-02-10.

9. *Hotel Customers Cheated of Rs 1 Cr; Four Held*, TIMES OF INDIA (June 22, 2008), https://timesofindia.indiatimes.com/city/pune/hotel-customers-cheated-of-rs-1-cr-four-held/articleshow/3152968.cms.

10. *The Morris Worm: 30 Years Since First Major Attack on the Internet*, FED. BUREAU OF INVESTIGATION (Nov. 2, 2018), https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218.

11. *Pegasus: Malware Found on Five Phones but Evidence Is Inconclusive, Says SC-Appointed Panel*, SCROLL.IN (Aug. 25, 2022), https://scroll.in/latest/1031257.

12. *Red Alert, Netizens!*, DATAQUEST (Sept. 14, 2004), https://www.dqindia.com/red-alert-netizens/.

13. Andrew Rossow, *Cyberbullying Taken to a Whole New Level: Enter the Blue Whale Challenge*, FORBES (Feb. 28, 2018), https://www.forbes.com/sites/andrewrossow/2018/02/28/cyberbullying-taken-to-a-whole-new-level-enter-the-blue-whale-challenge/.

14. *Supreme Court Stays HC Proceedings in Pleas of X Corp, Kunal Kamra & Others Against Sahyog Portal, Content Blocking Powers*, LIVELAW (Aug. 2026), https://www.livelaw.in/top-stories/supreme-court-stays-hc-proceedings-in-pleas-of-x-corp-kunal-kamra-others-against-sahyog-portal-content-blocking-powers-544774.

15. *Telangana Tops India in Cybercrime*, DECCAN CHRONICLE (Oct. 2025), https://www.deccanchronicle.com/southern-states/telangana/telangana-tops-india-in-cybercrime-1907213.

16. Geoff White, *Love Bug's Creator Tracked Down to Repair Shop in Manila*, BBC NEWS (May 3, 2020), https://www.bbc.com/news/technology-52458765.