CYBERCRIMES IN INDIA: LEGAL FRAMEWORK

Noor ul Ainain Nazir. Research Scholar,
Department of Law, University of Kashmir, Srinagar

ABSTRACT

Cybercrime in India has expanded rapidly with the widespread use of digital services, mobile payments, e-commerce, and social media. Cybercrimes in India have grown substantially in both scale and complexity as digital services, online communication, and electronic payments have become embedded in daily life. Cyber frauds refer to deceptive activities carried out through digital platforms such as unauthorized access, data theft, or online scams, which are often intended to cause financial loss to victims. This paper maps major categories of cyber offending, outlines the principal features of India's legal framework governing cyber offences and their regulations. Relying on figures from India's National Crime Records Bureau (NCRB) alongside official policy and institutional measures reported by the Government, the paper identifies trends in reported cybercrimes and explains why case counts may not capture the full extent of victimisation. The study concludes by suggesting policy directions to strengthen investigative capacity, improve victim support, and advance prevention through risk-informed regulation and cyber security-by-design. The paper concludes that while India's legal structure is sufficiently broad to address a wide range of cyber-enabled harms, operational bottlenecks in evidence readiness, coordination speed, and technical-to-legal translation remain central.

Keywords: Cybercrime: India, Information Technology Act 2000, NCRB, Judicial Interpretation.

I. INTRODUCTION

We live in the era of rapid digitalization and technological advancement is at its peak. According to Internet and Mobile Association of India (IAMAI's) latest edition of Internet in India report, India now has 958 million Active Internet Users (AIUs), reinforcing the country's position as one of the world's largest and fastest evolving digital markets. The report also reveals that rural India accounts for 57% of India's active internet users i.e. approximately 548 million active internet users.[1]

As of January 2023, India had 692 million internet users, with approximately 30.4% being children.[2] While this connectivity has brought many benefits, it has also created new challenges for everyday users and businesses alike. With our growing reliance on the internet, protecting our personal and organizational information has become essential. Whether you run a company, manage a business, or simply use the internet regularly, it's important to understand how to reduce risks, prevent cybercrime, and stay alert to the tactics used by cybercriminals. As technology advances, people depend more on the internet for nearly everything. It offers convenient access to services and opportunities from social networking and online shopping to storing data, studying online, and even working remotely all from the comfort of one place. Because the internet is now used in almost every part of life, its expansion has also led to the rise of cybercrimes.

Cybercrime refers to offences committed using computers, networks, or digital communications as either a target or a tool. "Cybercrime" is not a single statutory category under Indian law; rather, it includes a spectrum of offences where computers, networks, or digital communications are either the instrument of crime or the target. In practice, cyber offending often manifests as fraud-enabled impersonation (e.g., phishing and account takeover), misuse of credentials and identities, and harms that disproportionately affect vulnerable groups particularly women and children through image-based abuse, stalking, and related online intimidation.

This paper looks at unlawful acts in which a computer or technology is used as a tool. Many of these offenses are variations of traditional crimes carried out through information technology.

[1] Editorials, "India now has 958 million active internet users; 57% of these are from rural areas" *The Hindu*, Jan 29, 2026.
[2] Kemp, 2023.

Cybercrime is often categorized according to the target or subject of the crime. Cybercrime against individuals are directed at an individual or their property such as unauthorized access, online fraud, Cyber stalking, hacking, identity theft. Cybercrime targeting institutions or organizations include Data breaches, Cyber terrorism, Denial of service (DoS) attacks Cybercrime against society affect society as a whole, and they often impact young people and children the most. They include banned websites and harmful or illegal materials made available to the public through the internet. Examples of cybercrimes against society are child pornography, selling illegal items, forgery spamming.

II. Information Technology Act, 2000

The first cyber legislation on India i.e. the Information Technology Act, 2000 (IT Act, 2000) is a product of United Nation's General Assembly resolution passed January 30 of year 1997. This resolution was based on modal law of UNICITRAL for the adoption and implementation of - Electronic commerce.[3] India is a signatory of the Model Law, following which India passed the IT Act.

The primary objective of the IT Act, 2000 was to provide legal recognition for transaction carried out by means of electronic data interchange and other means of electronic communication, known as "electronic commerce".

The IT Act, 2000 has extra territorial operation or jurisdiction, the cyber space has no traditional borders. The crimes are committed beyond national borders, as the internet ensures anonymity.

Information Technology Act, 2000 was limited only to regulate e- commerce at the point of time initially, thus there was a need to address the cyber offences. The IT **(**Amendment Act 2008), included a separate part on cyber offences under chapter XI describe certain act as offences comprising fourteen sections ranging from 65 to 78.

III. Types Of Cybercrimes Under IT Act, 2000

a) **Hacking:** Unauthorised access/control of a computer system with intent to destroy, delete, or alter data. Punishment up to 3 years' imprisonment, or fine up to ₹5 lakh, or

[3] History of Cyber Law in India, http://www.indiancybersecurity.com (last visited on Jul 08, 2025).

both.[4]

b) **Identity Theft:** Using someone else's personal information (e.g., password, digital signature, Aadhaar, PAN) without permission to commit fraud or impersonate. Punishment up to 3 years' imprisonment and fine up to ₹1 lakh.[5]

c) **Cheating by Personation via Computer Resource:** Online impersonation and fraud (e.g., scam emails, fake profiles on social media, job scams). Punishment up to 3 years' imprisonment and fine up to ₹1 lakh.[6]

d) **Cyberstalking/Cyber Harassment:** Posting/transmitting private/sexual content without consent and stalking a person online/email/social media. Punishment up to 3 years' imprisonment and/or fine up to ₹2 lakh.[7]

e) **Obscene Material:** Uploading or distributing obscene/sexually explicit content electronically. Punishment: first offence up to 3 years and ₹5 lakh fine; repeat offence up to 5 years and ₹10 lakh fine.[8]

f) **Child Pornography:** Publishing, browsing, or downloading sexually explicit material involving children. Punishment up to 5 years' imprisonment and fine up to ₹10 lakh.[9]

g) **Cyber Terrorism:** Using computer systems to threaten India's unity, integrity, security, or sovereignty (e.g., attacks on defence/critical systems). Punishment may extend to life imprisonment.[10]

h) **Data Theft/Data Breach:** Unauthorised copying/downloading/extracting data. Liability: civil under Section 43 and criminal under Section 66; compensation may be claimed.[11]

i) **Denial of Service (DoS/DDoS):** Overloading a network/website to block legitimate users. Covered under: Section 43(f) and Section 66. Punishment up to 3 years'

[4] The Information Technology Act, 2000 (Act 21 of 2000), s. 66.
[5] The Information Technology Act, 2000 (Act 21 of 2000), s. 66C.
[6] The Information Technology Act, 2000 (Act 21 of 2000), s. 66D.
[7] The Information Technology Act, 2000 (Act 21 of 2000), s. 66E.
[8] The Information Technology Act, 2000 (Act 21 of 2000), s. 67.
[9] The Information Technology Act, 2000 (Act 21 of 2000), s. 67B.
[10] The Information Technology Act, 2000 (Act 21 of 2000), s. 66F.
[11] The Information Technology Act, 2000 (Act 21 of 2000), ss. 43 & 66.

imprisonment and/or fine.

j) **Tampering with Computer Source Documents**: Altering, destroying, or concealing source code needed to run programs. Punishment up to 3 years' imprisonment or fine up to ₹2 lakh, or both.[12]

IV. Scale of Reported Cyber Crime (NCRB-based trends)

At the national level, crime reporting is channelled through police registration and statistical compilation by the National Crime Records Bureau (NCRB). For example, government communications referencing NCRB data state that cybercrimes involving communication devices as medium/target increased from 52,974 cases in 2021 to 65,893 cases in 2022, and further to 86,420 cases in 2023.[13]

Official reported figures show a clear upward trend in cyber-crime cases in recent years (notwithstanding reporting biases and variations in enforcement/reporting practices). A government release citing NCRB reports that cyber-crime cases (communication devices as medium/target) were:

2021: 52,974

2022: 65,893

2023: 86,420[14]

These figures indicate both increased victimization and increased detection/reporting capacity. Importantly, a rise in FIRs can reflect multiple drivers: better public awareness, improved police handling, changes in classification, and shifting threat landscapes.

V. Judicial Interpretation: Critical Evaluation and Case Laws

Indian courts have played a significant role in interpreting cyber laws to protect children, often adopting a progressive stance to bridge legislative gaps. The Supreme Court, in a unanimous

[12] The Information Technology Act, 2000 (Act 21 of 2000), s. 65.
[13] https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=2003505 (last visited on Jul 11, 2026).
[14] https://www.pib.gov.in/PressReleasePage.aspx?lang=1&PRID=2241339&reg=3 (last visited on Jul 08, 2025).

decision in **Shreya Singhal v. Union of India**[15], held Section 66A of the Information Technology Act, 2000 to be unconstitutional. The Court found that it infringed the right to freedom of speech under Article 19(1)(a)[16] because it was drafted in broad and unclear terms, and therefore did not satisfy the "reasonable restrictions" requirement under Article 19(2). The Court also noted that the vague wording could deter people from making lawful statements, creating a "chilling effect" on free speech. The Court then clarified how Section 79 (intermediary liability) should operate. It explained that intermediaries would not be held responsible for third-party content unless they fail to comply with a lawful court order or government direction.

Finally, the Court upheld Section 69A, which empowers the government to order removal/blocking of certain content on grounds related to national security or public order. The Court considered this provision sufficiently specific and protected by safeguards, making it compatible with constitutional speech protections.

In **Sneha Kalita v. Union of India**[17], the Delhi High Court ordered the immediate removal of links to the Blue Whale Challenge, a game inciting self-harm among minors, under Section 69A of the IT Act. The court emphasized the state's duty to protect vulnerable populations, highlighting the need for proactive content moderation. Similarly, in **K.S. Putta swamy v. Union of India**[18], the Supreme Court recognized the right to privacy as a fundamental right under Article 21, extending its applicability to children's digital data. This ruling laid the groundwork for the Digital Personal Data Protection Act (DPDPA's) privacy safeguards.

However, judicial interpretations are inconsistent due to the lack of child-specific provisions. In **R. Rajagopal v. State of Tamil Nadu**[19]**,** the Supreme Court balanced privacy and free speech but failed to address minors explicitly, leading to ambiguity in cases involving children. **The National Insurance Company Ltd. v. IFFCO Tokio General Insurance Co. Ltd.**[20] case underscored corporate liability for data breaches, but its applicability to children's data remains limited. Courts often adopt a case-by-case approach, resulting in fragmented protections. The absence of fast-track courts for cybercrimes against minors further delays

[15] AIR 2015 SC.
[16] The Constitution of India.
[17] AIR Writ Petition (Civil) No. 000748/2017.
[18] AIR (2017) 10 SCC 1
[19] AIR (1994) 6 SCC 632.
[20] AIR (2016).

justice, undermining deterrence.

While courts have attempted to adapt existing laws to protect children, the lack of clear legislative guidance limits their efficacy. Judicial activism cannot substitute for comprehensive legislation, and the reliance on general statutes like the IT Act often fails to address the nuanced needs of minors in the digital space.

The Supreme Court of India, in **State of Punjab and Others v. M/S Amritsar Beverages Ltd. and Others,**[21] emphasized the complexity of dealing with cybercrimes and the gaps in the current legal framework.

Although India has legal provisions to address cybercrime, conviction rates remain very low. Courts frequently point to slow procedures, weak or incomplete investigations, and insufficient capacity within the criminal justice system. In most cybercrime cases, evidence is not collected effectively especially digital evidence, which demands technical handling and strict chain-of-custody practices.

Judges and investigators often rely on traditional legal approaches when dealing with highly technical cyber issues, which can lead to the digital evidence being misunderstood or undervalued. For instance, in hacking or data-breach cases, the failure to produce authenticated logs or credible forensic reports may result in acquittals. The situation is worsened by the lack of a dedicated cyber-judiciary and the limited availability of trained forensic experts within courts.

VI. CONCLUSION AND SUGGESTIONS

Cybercrimes in India reflect both a growing threat landscape and an enforcement system that is continuously tested by the technical and procedural demands of digital investigation. Substantively, the Information Technology Act and related criminal frameworks provide robust tools to criminalise cyber-enabled misconduct, including identity misuse, privacy-invasive conduct, and content-related offences. However, effective enforcement depends less on statutory text alone and more on the operational execution of evidence collection and proof-building in the early stages of a case. Investigations can fail or stall when digital evidence is not preserved promptly, when service-provider/platform records arrive late or in unusable

[21] AIR 2006 SC 2820.

forms, when electronic artefacts cannot be authenticated with sufficient integrity and chain-of-custody discipline, or when jurisdictional complexities delay attribution and legal access to records. These bottlenecks are compounded by variation in investigative and forensic capacity across states and investigative units, and by the difficulty of translating forensic outputs into precise legal ingredients required for conviction. Institutional coordination mechanisms and forensic assistance initiatives address some of these constraints, but the remaining priority is to make cybercrime enforcement more evidence-ready, faster, and more consistent from complaint intake to forensic triage, from inter-agency coordination to prosecution. Strengthening standardised digital evidence protocols, creating fast lanes for common cybercrime patterns, improving training for technical-to-legal translation, and reduce the enforcement gap between reported cyber harm and case outcomes. India's cyber law has evolved rapidly from virtually no digital-specific laws before 2000 to a robust, multi-layered framework today. The IT Act and its amendments helped bring structure, legal clarity, and accountability to India's digital ecosystem. Furthermore, IT Act's provision need to address emerging risks such as deep fakes and the misuse of generative AI. India should build a proactive, flexible cyber-legal framework rooted in transparency, accountability, and forward-looking technology. This approach should tackle cyber threats while protecting digital rights, enabling innovation, and strengthening international collaboration. With the right legal structure and strong institutional commitment, India can become a leader in cyber governance and ensure safety in the digital era. Given the extent of the cybercrimes, concluding this paper by listing the following suggestions.

1) The IT Act's provisions do not adequately address emerging risks such as deep fakes and the misuse of generative AI. In addition, the lack of mandatory age verification and clear content-moderation requirements for online platforms enables harmful content to spread, leaving children insufficiently protected.

2) There should be proper training of investigating agencies at district level, in every state of India. Establishment of adequate infrastructure in Cyber cells with proper high tech cyber security measures readiness to combat such incidents.

3) Awareness is most crucial and prevention measures workshops are to conducted in educational institutions by the cyber security experts.