The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

CYBER CRIMES IN INDIA: WHEN DOES IT BECOME A CRIMINAL OFFENCE?

LEGAL ANALYSIS OF INDIA'S EVOLVING CYBER LAW FRAMEWORK

Parikha jain

ABSTRACT

India recorded over one lakh cybercrime cases in 2024 for the first time, yet the precise point at which online conduct crosses from a civil wrong into a criminal offence remains widely misunderstood. This article examines that threshold through the dual framework of the Information Technology Act, 2000 and the Bharatiya Nyaya Sanhita, 2023. It identifies the five element courts consider necessary for criminal liability to attach, surveys the major offences and their punishments under Sections 66, 66C, 66D, 66F, 67A, 67B, and BNS Section 318, and analyses the constitutional limits on criminalisation as established in Shreya Singhal v. Union of India (2015). The article concludes with practical remedies available to victims and observations on the enforcement gaps that laws alone cannot close.

01 — INTRODUCTION

INDIA'S DIGITAL CRIME SURGE

India's digital economy is booming, but there's a dark side to all this progress. In 2024, cybercrime hit a record: for the first time ever, cases topped one lakh, with 1,01,928 reported — that's a big jump from 86,420 cases in 2023, up 17.9%.

But numbers don't tell the whole story. Here's what really matters: At what point does something you do online go from being just a civil issue to becoming a crime? It's a question that everyone—citizens, lawyers, students—wants answered. The answer isn't simple. It's shaped by the IT Act of 2000, the Bharatiya Nyaya Sanhita of 2023, and years of legal thinking and court decisions.

> *"Cybercrime is no longer a fringe threat — it has become India's fastest-growing category of registered crime, fuelled by rapid digital adoption and limited cyber literacy."*

02 — THE LEGAL FRAMEWORK

INDIA'S CYBER LAW ARCHITECTURE

India tackles cybercrime with two main laws. First, the Information Technology Act of 2000 lays out the groundwork. It's the country's core cyber law, running through 94 sections and 13 chapters. The Act nails down what counts as a cyber offence and sets penalties that range

from a fine to life in prison. In 2008, lawmakers gave it a serious upgrade, adding rules for newer problems like identity theft, cyber terrorism, and obscene content online.

Then there's the Bharatiya Nyaya Sanhita, 2023 (BNS), which took over from the old Indian Penal Code starting 1 July 2024. This one brings traditional crimes into the digital age. So if someone cheats, forges documents, or threatens others online — on social media or any digital platform — the law treats it just like it does when those things happen offline.

03 — THE CRIMINAL THRESHOLD CIVIL WRONG VS. CRIMINAL OFFENCE

The IT Act sets up two levels of liability. If someone hacks into a system, steals data, or spreads malware, Section 43 says they have to pay up—up to ₹1 crore—but they won't end up in jail for it. Jail time comes in under Chapter XI (Sections 65–78) and the BNS, where parliament has decided some offences deserve prison, not just a fine.

FIVE TRIGGERS FOR CRIMINAL LIABILITY

Drawing from judicial precedent and legislative intent, five elements consistently emerge before criminal liability can attach in a cybercrime case:

- First, the person has to actually do something illegal using a computer, system, or network.

- Second, they need to know what they're doing — or mean to do it. Most offences in the IT Act require actual knowledge or intent.

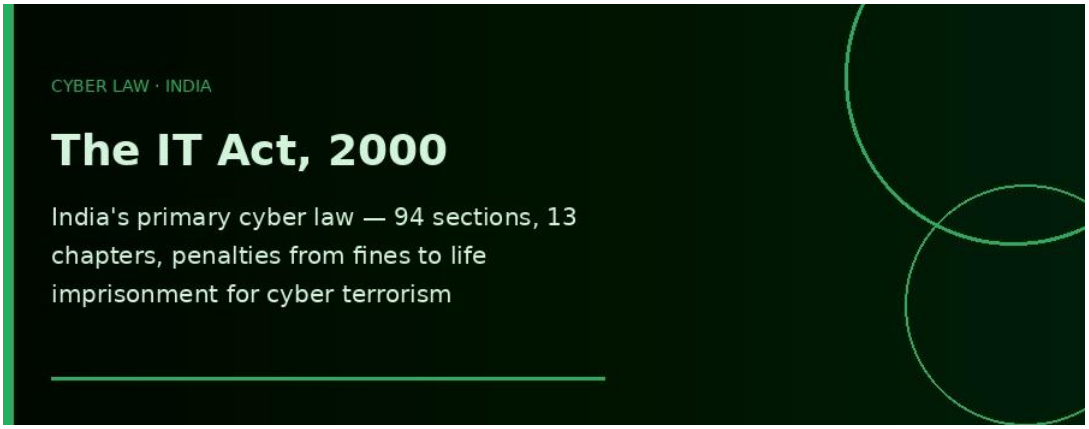
- Third, the action must fit one of the specific crimes outlined in the IT Act (Sections 65 to 78) or under the BNS.

- Fourth, the harm caused needs to be serious enough, like causing damage, gaining something dishonestly, spreading obscene material, or threatening national security.

- Finally, the crime should be categorized as cognizable. For most IT Act offences with more than three years' potential jail time, police can arrest without a warrant.

04 — MAJOR CRIMINAL OFFENCES

WHEN DOES EACH ACT BECOME A CRIME?



Section 66 — Hacking (Computer-Related Offences)

Section 66 — Unauthorised Access, Data Destruction, Malware

You break the law here if you're acting dishonestly or fraudulently—like sneaking into someone's data, destroying files, or unleashing malware when you shouldn't. If you just stumble in by accident, that doesn't count.

Punishment: You could face up to 3 years in jail, or pay a ₹5 lakh fine, or sometimes both.

Section 66C — Identity Theft

This one's about using someone else's electronic signature, password, or any other unique ID. It hits especially hard with SIM-swap frauds and account takeovers—basically, pretending to be someone you're not for personal gain.

Punishment: Up to 3 years imprisonment and a ₹1 lakh fine.

Section 66D — Cheating by Personation

If you use a computer or phone to pretend you're another person—maybe setting up a phishing site, making fake customer care calls, or spoofing emails—you're in violation.

Punishment: Up to 3 years in jail, or a ₹1 lakh fine, or both.

Section 66F — Cyber Terrorism

Section 66F carries the most serious charge in India's cyber law framework. If online actions threaten India's unity, integrity, or security, or block access to critical information, this provision applies.

Punishment: Life imprisonment.

Sections 67A/67B — Online Obscenity & Child Exploitation

Anyone who publishes, transmits, or causes to be published or transmitted explicit material — including child sexual abuse material online — falls under these sections. Mere passive browsing, without downloading or distribution, is not explicitly criminalised under Section 67B, though active engagement with such content may attract related pzrovisions. These are cognizable offences, so police don't need a warrant to act.

Punishment: Up to 7 years in prison and ₹10 lakh fine if convicted again.

BNS Section 318 — Online Cheating & UPI Fraud

This section covers digital scams—UPI fraud, investment scams, fake payment links, and so on. It's been heavily used in 2024 as online cheating grows.

Punishment: Up to 7 years in jail, plus a fine.

05 — LANDMARK CASE

Shreya Singhal v. Union of India (2015) fundamentally reshaped cyber law in India.

The Supreme Court struck down Section 66A of the IT Act, holding it unconstitutional to criminalise 'offensive' online messages. The Court found the provision overbroad and in direct conflict with the right to free speech under Article 19(1)(a). Its ruling established a clear standard: criminal cyber offences must be defined with precision — vague language will not withstand constitutional scrutiny. The case arose after two women were arrested in 2012 for a Facebook post commenting on the city shutdown following the death of Bal Thackeray. That arrest became a landmark moment for digital rights in India.

> *"Vagueness in criminal law is constitutionally impermissible. A citizen must know, in advance, what acts the law forbids. — Supreme Court of India, Shreya Singhal v. UoI (2015)"*

06 — VICTIM REMEDIES

WHAT CAN YOU DO IF YOU'RE A VICTIM?

1. Go to the National Cyber Crime Reporting Portal at cybercrime.gov.in. You can file a complaint there any time, day or night—no need to visit a police station. Use this for matters such as financial fraud, cyberstalking, or cases involving child exploitation.

2. Call the helpline at 1930. This hotline works all over India. If someone just stole your money online, call them right away—they can help freeze transactions fast.

3. If you're dealing with a serious cybercrime (anything under the IT Act with a punishment of more than three years), you have the right to file an FIR at the Cyber Crime Cell in your state. Don't let anyone tell you otherwise—this is your right.

07 — CONCLUSION

We live in a world where being online is no longer optional, and that means understanding the legal landscape matters for everyone. India's cyber laws—starting with the IT Act from 2000 and now bolstered by the BNS in 2023—set up a strong framework for tackling digital crime. Different crimes have different triggers: some focus on whether someone acted dishonestly, others require actual knowledge of wrongdoing, and then there's cyber terrorism, which looks at intent to damage the nation itself.

The numbers are difficult to overlook. Cybercrime cases in India just crossed the one-lakh mark for the first time, and fraud accounts for a striking 72% of that—almost 74,000 out of over 1,00,000 cases. Yet conviction rates in cybercrime cases remain low, cyber cells in many states are understaffed, and jurisdictional complexity continues to slow prosecution. Laws on the books alone are not enough. Enforcement agencies, court systems, and above all, basic digital literacy among citizens, must keep pace with the speed at which new online threats emerge.

Ignorance of the law is not a defence — and that applies as much online as it does offline. For legal professionals, the overlap between the IT Act and the BNS is not a footnote to be skimmed; it demands precision, current knowledge, and careful attention at every stage of practice.

BLUEBOOK CITATIONS

Legal References

[1]	The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India), as amended by the Information Technology (Amendment) Act, 2008, No. 10, Acts of Parliament, 2009 (India).
[2]	The Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023 (India) (enforced July 1, 2024).
[3]	Shreya Singhal v. Union of India, (2015) 5 SCC 1 (India).
[4]	Kalandi Charan Lenka v. State of Odisha, (2017) Cri LJ 3055 (Ori. HC) (India).
[5]	National Crime Records Bureau, Crime in India 2024, Ministry of Home Affairs (May 2026).
[6]	Int'l Comparative Legal Guides, Cybersecurity Laws and Regulations — India 2025 (Nov. 6, 2024), available at iclg.com.
[7]	Manorama Yearbook, Explainer — IT Act, 2000 (Mar. 16, 2024), available at manoramayearbook.in.
[8]	LawSection.in, Key Provisions — Cyber Crimes Under BNS, 2023 (Mar. 31, 2026), available at lawsection.in.