



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

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

CYBER CRIME AND LEGAL REMEDIES

~ *GUGASRIPRIYA SIVAGAMI RAVI*

It usually begins with something small, A message from an unknown number asking you to verify your bank details with a link promising a refund you never expected or a stranger's profile suddenly messaging your family members using your photograph. By the time the victim realises what has happened, money has left their account, their identity has been borrowed for someone else's fraud or their private pictures are circulating without consent. Cybercrime rarely announces itself; it slips in through the same convenience that makes digital life so attractive. As more of our banking, relationships and work move online, the law has had to catch up with a criminal who no longer needs to enter a home to rob it.

Cybercrime, in the simplest sense, is any offence in which a computer, network, or digital device is either the target or the tool. It ranges from financial fraud through phishing and UPI scams, to hacking, ransomware, data theft, cyberstalking and the non-consensual circulation of intimate images. What makes these offences distinct is not only their technical method but their reach: a single act, launched from one device can victimise thousands of people across states and even countries within minutes¹. Indian law has therefore had to build a framework wide enough to catch conduct that traditional criminal statutes drafted long before the internet were never designed to address.

The primary statute governing this space is the Information Technology Act, 2000, enacted to give legal recognition to electronic records and digital signatures while simultaneously criminalising misuse of computer systems². Section 43 creates civil liability for unauthorised access, data theft, and the introduction of viruses, entitling the victim to compensation³. Sections 65 and 66 criminalise tampering with source code and hacking, while Section 66C

¹ Laws, Types and Legal Remedies, Delhi Law Academy (2026); National Crime Records Bureau, Crime in India Report (2023–24 ed.).

² Information Technology Act, No. 21 of 2000, INDIA CODE (2000).

³ Information Technology Act, No. 21 of 2000, SS 43, INDIA CODE (2000).

penalises identity theft through misuse of passwords or unique identification features and Section 66D specifically targets cheating by personation using a computer resource, the provision most often invoked against online scam artists⁴. Section 67 addresses the publication of obscene material in electronic form.

These provisions do not operate in isolation; the Bharatiya Nyaya Sanhita, 2023, which replaced the Indian Penal Code continues to supply offences such as cheating, criminal intimidation and defamation that frequently overlap with cybercrime committed through digital means⁵.

The law in this area has also been shaped significantly by the judiciary. In *Shreya Singhal v. Union of India*, the Supreme Court struck down Section 66A of the IT Act, which had criminalised sending grossly offensive or annoying messages online holding that its vague and undefined terms permitted arbitrary enforcement and had a chilling effect on the freedom of speech and expression guaranteed under Article 19(1)(a) of the constitution⁶. The judgement also clarified the extent of an intermediary's liability under section 79 holding that platforms are obliged to remove content only upon receiving a court order or a notification from the appropriate government authority rather than on the basis of private complaints alone. The decision remains a cornerstone of India's digital rights jurisprudence illustrating that even as the state seeks to police cyberspace, it must do so within constitutional limits.

For a victim, the more pressing question is rarely constitutional theory but a practical one: what can actually be done once the fraud has happened? Indian law offers a layered set of remedies. The first and most immediate step is to preserve evidence, screenshots, transaction records, before reporting the incident on the National Cyber Crime Reporting Portal or through the 1930 helpline, both of which route complaints to the relevant state cyber cell⁷. Where the offence is criminal in nature, the victim may lodge a First Information Report at the local police station, citing the specific sections of the IT Act involved; if the police decline to register the complaint, the complainant retains the right to approach a Judicial Magistrate under section 156(3) of the

⁴ Information Technology Act, No. 21 of 2000, SS 65–66, 66C, 66D, INDIA CODE (2000).

⁵ Bharatiya Nyaya Sanhita, No. 45 of 2023, INDIA CODE (2023).

⁶ *Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1 (India).

⁷ How to File a Cybercrime Complaint in India: Complete Guide, JuristCo (2026).

Code of Criminal Procedure to direct an investigation⁸. Parallel to the criminal process, a victim who has suffered financial loss may approach the Adjudicating Officer appointed under the IT Act for compensation under Section 43, offering a civil route that does not require proving guilt beyond reasonable doubt.

None of this makes the system frictionless, Cybercriminals frequently operate across borders hide behind rented SIM cards and mule bank accounts and exploit gaps between jurisdictions that no single state police force can close alone. Digital evidence is easy to alter and can vanish before an investigation catches up and many victims particularly those targeted through romance scams or intimate image abuse hesitate to report out of embarrassment allowing offenders to repeat the same scheme against others. Strengthening cyber forensics capacity training police personnel and building public awareness of the reporting portal remain as important as the statutory text itself.

Cybercrime is not a distant, technical problem confined to specialists; it is a lived risk for anyone who owns a smartphone. India's legal framework anchored in the Information Technology Act and refined by judgements like *Shreya Singhal* gives victims real avenues for redress but the law can only work as fast as people are willing to use it. Knowing where to report, what evidence to preserve and which remedy to pursue is increasingly as essential a life skill as locking one's front door.

⁸ Code of Criminal Procedure, No. 2 of 1974, ss 156(3), INDIA CODE (1974).