

CYBER CRIMES AND CRIMINAL LIABILITY IN INDIA

Offences, Attribution and Electronic Evidence under the IT Act, 2000, the Bharatiya Nyaya Sanhita, 2023 and the Bharatiya Sakshya Adhiniyam, 2023

H R Rathna Bai

LL.B. (Hons.)

SCSVMV University, Kanchipuram, Tamil Nadu, India

Abstract : Digital systems are both targets of criminal attacks and instruments through which familiar offences are committed. Indian law responds through a combination of the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023 and rules governing electronic evidence. This article examines how those frameworks allocate criminal responsibility for unauthorised access, identity misuse, online deception, digital forgery and related conduct. Using doctrinal analysis, it distinguishes proof that an incident occurred from proof that an accused committed the relevant offence with the required mental element. It also evaluates intermediary and corporate liability, the treatment of electronic records and the practical limits of cross-border enforcement. The article argues that broader criminalisation alone cannot resolve difficulties of attribution and proof. Effective enforcement requires reliable preservation of digital material, offence-specific investigation, trained institutions and constitutional safeguards. A coordinated approach should protect victims and digital infrastructure while avoiding liability based merely on account ownership, corporate designation or unpopular online expression.

Index Terms - cybercrime; criminal liability; Information Technology Act; Bharatiya Nyaya Sanhita; digital evidence; attribution; intermediary liability.

I. INTRODUCTION

Digital communication has made it possible to transact, study and access public services without physical proximity. The same separation between people, devices and locations creates opportunities for wrongdoing. An offender may impersonate an institution, interfere with a remote system or circulate a fabricated record while the relevant evidence remains distributed across several providers.

The expression cybercrime is useful as an umbrella term, but it does not identify a single offence. A computer may be attacked, used to facilitate a conventional crime or hold evidence of wrongdoing. These roles can overlap within one incident. Legal analysis must therefore move beyond the label and identify the precise prohibited conduct.

This article argues that the central challenge is connecting statutory ingredients with dependable evidence. Identifying a suspicious device, transaction or account is only one part of that task. Criminal responsibility also requires a legally sufficient connection between the accused, the conduct and the mental element of the offence.

The discussion brings legislation, investigation and individual rights into an integrated analysis. Its principal contribution is to distinguish three questions that are often combined: what offence the conduct discloses, who is legally responsible, and how the relevant facts can be proved.

II. METHODOLOGY AND SCOPE

The research is doctrinal and analytical. It examines selected provisions of the Information Technology Act, 2000 (IT Act), the Bharatiya Nyaya Sanhita, 2023 (BNS), the Bharatiya Sakshya Adhiniyam, 2023 (BSA) and judicial decisions concerning expression, electronic evidence and personal responsibility.

The inquiry is confined primarily to Indian criminal law. It does not include interviews, surveys or a statistical assessment of crime rates. Illustrations are hypothetical. Recommendations concerning training, preservation and coordination are proposals drawn from the legal problems analysed, rather than claims that particular interventions have already produced measurable results.

The discussion is selective rather than an inventory of every technology-related offence. It focuses on the relationship between general criminal law, computer-specific provisions and evidentiary safeguards. Older judgments are explained in the context of the statutes they interpreted; they are not described as rulings directly construing the BNS or BSA.

III. IDENTIFYING THE OFFENCE

A. Unauthorised Access and Interference

The distinction between a civil contravention and a criminal offence must be maintained. Section 43 of the IT Act addresses specified acts performed without the permission of the relevant owner or person in charge. Section 66 criminalises the acts referred to there when performed dishonestly or fraudulently, with imprisonment up to three years, fine up to five lakh rupees, or both [1, §§ 43, 66].

Consequently, the occurrence of access or damage does not dispense with the relevant criminal mental element. Permission, its scope and the accused's conduct must be established. An authorised security test and a malicious intrusion may involve superficially similar technical operations but require different legal conclusions.

An investigation should identify the actual act alleged, such as access, copying, disruption or alteration, instead of relying only on the word hacking. That approach clarifies which evidence is necessary and allows the defence to understand the case it must answer.

B. Identity Misuse and Online Deception

Section 66C addresses fraudulent or dishonest use of another person's electronic signature, password or other unique identification feature. Section 66D concerns cheating by personation through a communication device or computer resource. Both provide imprisonment up to three years and liability to fine up to one lakh rupees [1, §§ 66C–66D].

These provisions protect related interests but have different ingredients. Misuse of credentials is not identical to inducing a victim through a false identity. For example, a false message purporting to come from a bank must be examined for the deception and response alleged; its electronic form does not itself prove every component of cheating.

The BNS may also become relevant. Section 318 addresses cheating and its aggravated forms, while section 319 addresses cheating by personation. A charge must identify the applicable subsection, the inducement and the necessary consequence rather than treat every unsuccessful online transaction as criminal fraud [2, §§ 318–319].

C. Digital Forgery and Harmful Communications

Electronic fabrication can also engage the BNS provisions on false records and forgery. Sections 335 and 336 require a legally false document or electronic record and the specified intention. Section 340 separately addresses fraudulent or dishonest use as genuine with knowledge or reason to believe that the record is forged [2, §§ 335–336, 340].

A fabricated electronic certificate may therefore raise forgery issues even before it successfully deceives a recipient. A merely untrue assertion in an authentic document, however, does not automatically satisfy the statutory test of making a false record. Authorship, authority and material alteration require separate examination.

Online threats, demands and monitoring may attract other offences. Depending on the facts, BNS section 308 on extortion, section 351 on criminal intimidation and section 78 on stalking may be relevant. Section 78 is specifically framed around conduct by a man towards a woman and includes monitoring her electronic communications; it should not be presented as a general offence covering every form of online harassment [2, §§ 78, 308, 351].

D. Content Offences and Cyber Terrorism

The IT Act contains distinct provisions concerning obscene electronic material, sexually explicit material and specified material or conduct involving children under sections 67, 67A and 67B. Their separate statutory requirements matter. The fact that a post is offensive, objectionable or widely criticised does not by itself establish one of these offences [1, §§ 67–67B].

Section 66F provides for cyber terrorism and permits punishment extending to life imprisonment. Its demanding statutory conditions must be established; a disruptive incident is not automatically terrorism merely because it affects an important system. Serious labels cannot replace proof of the prescribed conduct, intention and other elements [1, § 66F].

IV. CRIMINAL RESPONSIBILITY AND ATTRIBUTION

A. Conduct and Mental Element

Criminal liability depends on the particular offence rather than on a single mental standard applicable to all cyber incidents. Some provisions require dishonesty or fraud, while others use knowledge, intention or another specified condition. The prosecution must connect the evidence to the language of the charge.

Attribution is a related but distinct problem. An account registered in a person's name may have been shared, compromised or accessed remotely. A network identifier can indicate a technical connection without conclusively identifying the human actor. Such possibilities require investigation, not an automatic assumption of either guilt or innocence.

A stronger case considers communications, device activity, access history, financial movements and other legally obtained evidence together. Each item must be evaluated for what it actually establishes. A payment to an account, for instance, may show where money moved without conclusively establishing who designed the deception.

B. Participation by Several People

A digital incident may involve people who create false material, send messages, supply access or receive funds. Their functions should be distinguished. Liability for participation, abetment or conspiracy depends on the elements of the applicable law, not merely on proximity to the principal offender. The IT Act expressly addresses abetment and attempts in sections 84B and 84C [1, §§ 84B–84C].

This distinction is particularly important for intermediaries such as service providers and for people whose accounts were used without authority. Assistance must not be inferred solely from the existence of a technical service or a contact between participants. Conversely, using separate roles does not prevent liability where the necessary involvement is proved.

C. Corporate and Intermediary Responsibility

Section 85 of the IT Act provides a statutory framework for company-related contraventions, including responsibility associated with control of the company's business and specified consent, connivance or neglect. Its proviso also recognises defences concerning lack of knowledge or due diligence. Corporate office alone should not replace analysis of these conditions [1, § 85].

The broader principle is illustrated by *Sunil Bharti Mittal v. Central Bureau of Investigation*. In proceedings arising from alleged spectrum-allocation irregularities, the Supreme Court rejected the automatic attribution of a company's alleged acts to its controlling officers merely through their position. Personal involvement with the necessary mental element or a statutory basis for vicarious liability is required [3].

Intermediary liability raises a different question. IT Act section 79 provides conditional protection concerning third-party information, subject to statutory requirements and exclusions. Losing that protection does not, by itself, prove the ingredients of an underlying criminal offence. The alleged basis of liability must still be identified [1, § 79].

V. ELECTRONIC EVIDENCE AND PROOF

A. Admissibility Is Not Authenticity

The BSA recognises electronic and digital records. Sections 61–63 address their legal treatment and proof, including the conditions for computer outputs and the certificate framework under section 63. A record's electronic format does not exclude it, but neither does its admission automatically establish its authenticity or truth [4, §§ 61–63].

A screenshot may depict a message without identifying its sender reliably. A file may contain an apparent signature without demonstrating genuine authorisation. Courts must distinguish the admissibility of an exhibit from the inferences that may properly be drawn from it.

B. Lessons from *Anvar* and *Arjun Panditrao*

Anvar P.V. v. P.K. Basheer arose from an election dispute involving electronic material. The Supreme Court stressed the special statutory route for proving electronic outputs under section 65B of the former Evidence Act, rather than bypassing it through general secondary-evidence rules [5].

In *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, another election-related dispute, a larger Bench reaffirmed the certificate requirement for the electronic-output route and clarified the distinction involving production of an original electronic record. It also addressed obtaining the certificate through appropriate judicial assistance [6].

These cases explain why reliable electronic proof needs more than a printout bearing an allegation. They interpreted the earlier Evidence Act. Their reasoning provides background for current practice, but the requirements of BSA section 63 must be examined directly where that statute applies. Transitional proceedings also require attention to the BSA's savings provision [4, §§ 63, 170(2)].

C. Preservation and Forensic Interpretation

Investigators should preserve relevant devices or records through lawful procedures and document collection, copying, transfer and examination. A consistent chain of custody helps explain how an exhibit reached the court and whether it remained intact. Where available, original file formats and relevant metadata may reveal information absent from a printed image.

Hash values can help verify whether a particular digital copy has changed, but do not prove that its original contents were truthful or identify its author. Likewise, forensic software produces findings that require interpretation. The examiner should explain the method, the material examined and the limits of the conclusion.

Preservation must also remain targeted. Collecting every item on a device without considering relevance can expose unrelated private information and burden review. Clear procedures for access, retention and disclosure would support both effective prosecution and a fair opportunity to challenge the evidence.

VI. CONSTITUTIONAL BOUNDARIES

In *Shreya Singhal v. Union of India*, the Supreme Court struck down IT Act section 66A for violating freedom of expression. The Court addressed vagueness and overbreadth and distinguished discussion and advocacy from incitement in its constitutional analysis. Section 66A cannot be presented as an available offence against offensive online messages [7, ¶ 119].

The judgment also upheld section 69A and its blocking framework and read down the actual-knowledge requirement in section 79(3)(b). Its treatment of intermediaries demonstrates that enforcement powers and third-party responsibility must operate within legal safeguards rather than through an unrestricted duty to suppress disputed expression [7].

The importance of the decision extends beyond one invalidated provision. Cybercrime policy must differentiate harmful conduct defined by law from expression that is merely unpopular. At the same time, the judgment does not immunise genuine threats, fraud or other offences whose ingredients are independently established.

Constitutional protection and victim protection should therefore be pursued together. Precise charges, reasoned orders and reliable evidence are means of making enforcement legitimate, not obstacles that can be set aside whenever technology creates investigative difficulty.

VII. JURISDICTION AND ENFORCEMENT CHALLENGES

The IT Act extends to specified conduct outside India where the statutory connection with a computer, system or network located in India is satisfied. BNS section 1 also contains provisions concerning extraterritorial application, including specified offences targeting computer resources in India. These are legal bases for jurisdiction, not guarantees that evidence or an accused abroad can immediately be obtained [1, § 75], [2, § 1(4)–(5)].

A provider may hold relevant information under another country's legal system. Investigators may then need preservation requests, cooperation between competent authorities or formal assistance. The existence of domestic jurisdiction and the practical ability to enforce it must be kept separate.

Delay can reduce the usefulness of available records, while large volumes of data can obscure the evidence that matters. A structured plan should identify the alleged offence, the material needed to prove it and the lawful route for obtaining that material. Requests framed too broadly may be slower and harder to justify.

Emerging technologies intensify familiar attribution problems. A synthetic voice or image can make an impersonation persuasive, but does not change the need to prove deception and the relevant actor's role. Encrypted communication and remote storage may complicate access, yet their use is not itself proof of criminal intent.

VIII. RECOMMENDATIONS

First, investigative training should link technical findings to offence-specific legal requirements. Officers should be able to distinguish credential misuse, personation, false-record creation and knowing use rather than treat them as interchangeable forms of fraud.

Second, electronic-evidence planning should begin early. Investigators and prosecutors should identify relevant sources, arrange lawful preservation and consider the required certificates before trial. Remedial applications cannot always recover records that were never preserved.

Third, forensic capacity should include quality assurance and understandable reporting. Courts need explanations of what a method establishes and what uncertainty remains. Both parties should have a meaningful opportunity to examine the basis of a technical conclusion.

Fourth, institutional procedures should support proportionate collection and secure handling of personal information. Access controls, documented retention and reasoned disclosure decisions can reduce unnecessary exposure while preserving relevant evidence.

Fifth, cooperation with service providers and foreign authorities should use clear legal channels and carefully framed requests. Domestic competence to prosecute must be supported by practical arrangements for preservation, production and witness assistance.

Finally, prevention should complement prosecution. Institutions can verify changed payment instructions through independent channels, maintain appropriate audit trails and educate users about impersonation. Such measures reduce opportunities for deception without shifting legal responsibility from offenders to victims.

IX. CONCLUSION

India's framework addresses cyber wrongdoing through computer-specific offences, general criminal law and rules governing electronic proof. The central legal task is to identify the correct provision, connect the accused to the prohibited conduct and establish its required mental element. A device, account or corporate title is not an adequate substitute for that analysis.

The IT Act and BNS can address different aspects of the same incident, while the BSA regulates how relevant electronic material is proved. Judicial decisions reinforce the need for careful evidence and constitutional boundaries. They also show why neither a broad crime label nor the existence of a digital exhibit determines liability by itself.

Effective reform should therefore strengthen investigation, preservation and reasoned adjudication alongside prevention. Technical competence and procedural fairness support the same objective: holding the responsible person accountable on dependable evidence while protecting those whose connection with an incident has not been proved.

X. REFERENCES

- [1] Information Technology Act, No. 21 of 2000 (India).
- [2] Bharatiya Nyaya Sanhita, No. 45 of 2023 (India).
- [3] *Sunil Bharti Mittal v. Central Bureau of Investigation*, (2015) 4 S.C.C. 609 (India).
- [4] Bharatiya Sakshya Adhiniyam, No. 47 of 2023 (India).
- [5] *Anvar P.V. v. P.K. Basheer*, (2014) 10 S.C.C. 473 (India).
- [6] *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 S.C.C. 1 (India).
- [7] *Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1 (India).

Copyright & License:

© Authors retain the copyright of this article. This work is published under the Creative Commons Attribution 4.0 International License (CC BY 4.0), permitting unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.