CYBERCRIME AND LEGAL REMEDIES: EVALUATING INDIA'S EVOLVING LEGAL FRAMEWORK

AI Disclosure Statement :

The author used an AI-assisted writing tool solely for language editing, grammar refinement, and formatting assistance. All legal research, analysis, case law interpretation, arguments, and conclusions presented in this manuscript are the author's own work.

Abstract

The past few years have seen the increased and continuous development of technology, which also contributed to the occurrence of new forms of cybercrime, presenting new challenges for law enforcement agencies and courts. Cybercrime such as identity theft, online fraud, cyberstalking, data breach, and online harassment has become a cross-border issue. The paper aims to review the changing legal provisions of India to respond to such types of cybercrime. The study focuses on the Information Technology Act, 2000, the Bharat Nyaya Sanhita, 2023, and other regulations in this sphere. The analysis presents the existing legal tools available to victims, investigation methods, the nature and admissibility of electronic evidence, and the agencies involved in combating cybercrime. The paper also discusses practical issues affecting successful implementation, including jurisdiction issues, lack of technology, underreporting, verification and attribution issues, and problems with the institutional capacities. The author state that although the country has made a huge progress in improving its laws regarding cybercrime, their effectiveness depends not only on more crimes being defined as criminal offences but also on improving the investigation abilities and cooperation between relevant agencies and using electronic evidence.

KEYWORDS

Cybercrime, Information Technology Act, Digital Evidence, Cybersecurity, Data Protection, Legal Remedies.

I. Introduction

Digital technology has changed drastically the way people communicate, conduct financial transactions, store information and obtain public and other services. This very technology also provides new tools for crime. Cybercrime is not limited now only to traditional hacking. It includes crimes against computers, crimes committed with the help of computers, illegal use of personal information, online financial scams, online harassment, sexual crimes and crimes against organizations and infrastructure. [1]

Due to this, the legal nature of cybercrime is complicated. For example, a computer fraud could be an illegal use of a computing machine, stealing identity, fraud by impersonation and corrupt delivery of goods. Thus, such actions could apply many special laws as well as general Criminal Code provisions. The current situation in India corresponds to this overlap. Information Technology Act 2000 (IT Act) is the main special law regulating computer crimes while Bharatiya Nyaya Sanhita 2023 (BNS) describes crimes like fraud and impersonation regardless of the means of committing them. [2]

The arrival of the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS) and the Bharatiya Sakshya Adhiniyam, 2023 (BSA) has changed the scenario of how criminal cases are handled legally. Furthermore, while the Digital Personal Data Protection Act, 2023 (DPDP Act) and the Digital Personal Data Protection Rules, 2025 have established an independent system regarding safeguarding and processing of data.[3]

Therefore, the question is more about whether India has enough provisions for cybercrime than just the fact that there are enough laws. The critical point is that law does not fail due to lack of provisions, but it fails due to the fact that implementation is not effective.

1. Information Technology Act, No. 21 of 2000.
2. Information Technology Act, No. 21 of 2000, §§ 43, 66C–66F; Bharatiya Nyaya Sanhita, No. 45 of 2023, §§ 318–319.
3. Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023; Bharatiya Sakshya Adhiniyam, No. 47 of 2023; Digital Personal Data Protection Act, No. 22 of 2023.

II. India’s Substantive Legal Framework

A. The Information Technology Act, 2000

The backbone of the framework of specialized cyber law in India rests on the IT Act. The 43rd section of the Act talks about civil liability imposed on particular acts involving computers and computer systems like unauthorized access and data copying. Historically, section 43A has provided for compensation in case of negligence by the body corporate in ensuring the security of sensitive personal data or information. [4]

The criminal liability has been dealt in a more efficient manner in chapter XI of the IT Act. The 65th section of the Act penalizes the tampering of computer sources. The 66th section of the Act converts the acts mentioned in the 43rd section as a criminal offense if performed dishonestly. Sections 66C and 66D become more important in the current times in terms of cyber crime. Section 66C deals with identity theft while 66D deals with cheating by impersonation through the use of a computer resource or communication device.[5] Section 66E deals with the violation of privacy whereas section 66F is concerned with cyber terrorism. The 67th to 67B sections of the Act deal with "obscene, sexually explicit and child sexual material in electronic form."[6]

The Act also adds tips about regulation and cybersecurity. Section 69 deals with interception, monitoring, or decryption in certain situations; section 69A deals with the blocking of certain information; section 70 deals with secure systems; and section 70B recognizes CERT-In, the Indian Computer Emergency Response Team, as the national agency for responding to cyber-security incidents.[7]

The extent of these provisions proves how India has recognized cybercrime as a specific legal issue. The more complicated issue is the relation between specialized cybercrimes and common crimes. Digital technology usually only serves as a tool for committing crimes. Thus, an effective response should not rely entirely on the IT Act.

4. Information Technology Act, No. 21 of 2000, §§ 43, 43A.
5. Id. §§ 65–66D.
6. Id. §§ 66E–67B.
7. Id. §§ 69, 69A, 70, 70B.

B. The Bharatiya Nyaya Sanhita, 2023

The BNS law replaces the Indian Penal Code of 1860 and bolsters the concept of overlapping. Under this code, Section 318 pertains to cheating and Section 319 pertains to cheating by impersonation.[8] The application of this law has direct implications when it comes to cyber crimes such as scams, phishing, creating false profiles etc.

The overlap in laws is of legal significance in itself. The person committing deception online may not strictly follow any of the laws that are specifically part of the IT Act, whereas the use of e-mails, WhatsApp etc. does not imply that the crime committed has necessarily assumed the form of a cyber-crime. The BNS would be applicable to criminal wrongs performed, whereas the IT Act would apply in all matters related to misuse of computing resources.

The said application of the two laws is advantageous as it pre-empts technological change from making the traditional crimes ineffective. However, it calls for the investigators and the prosecution to fully understand how the two laws interplay and interact with each other. It is more a question of coordination rather than pure change in legislation.

III. Data Security and Cyber Crime

The DPDP Act is related to but different from the position. It cannot be considered a general legislative act concerning cyber crime. Its main aim is to control the processing of digital personal data while recognizing the personal interest of the individual in terms of protecting the data and legal requirements to process this data.[9]

The Act introduces the obligations for Data Fiduciaries, as well as rights and obligations of Data Principals, provisions for Significant Data Fiduciaries, and Data Protection Board of India. The Section 33 stipulates the monetary consequences in case of serious breaches.[10]

8. Bharatiya Nyaya Sanhita, No. 45 of 2023, §§ 318–319.
9. Digital Personal Data Protection Act, No. 22 of 2023, Long Title.
10. Id. § 33.

The significance of this framework grew considerably after the issuance of the Digital Personal Data Protection (DPDP) Rules in 2025. The Central Government dated 13 November 2025 issued the notifications stating that the different provisions of the act would be enforced in stages, while the Rules were issued on 14 November 2025.[11]

The difference of data protection and cybercrime is still very relevant. A data breach could trigger obligations related to data protection, unauthorized access could fall under the IT Act, and fraudulent use of stolen information could lead to committing an offense under the BNS or IT Act. This illustrates that the same action can have different legal consequences.

Therefore, this demonstrates the significant structural characteristic of the Indian cyber law, the issue of cybercrime cannot be understood with the help of only one law.

IV. Procedural and Evidentiary Remedies

A. Jurisdiction

Cybercrime challenges traditional notions of territorial jurisdiction. For example, in the case of online financial fraud, the crime may have taken place with involvement of a victim living in one state, a bank account from another, a perpetrator from yet another territory and an Internet service provider in yet another country.

The BNSS law partially addresses this issue. Section 202 states that the investigative and trial nature of the crime of cheating conducted via electronic communication allows for the crime's investigation and trail in the place where the electronic communication is sent or received, and jurisdiction is granted in cases where property is delivered by the victim or received by the perpetrator.[12]

11. Ministry of Electronics & Information Technology, Notification No. G.S.R. 843(E), Nov. 13, 2025; Ministry of Electronics & Information Technology, Digital Personal Data Protection Rules, 2025 (Nov. 14, 2025).

12. Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023, § 202.

This legal innovation is indeed good for local cyber fraud cases because it implies that electronic communication leaves the boundaries of the usual territorial jurisdiction. However, it does not guarantee the investigation's success in the case of real transnational crimes since, if the evidential material is located abroad, the Indian prosecution and investigation authorities can act only with the help of international cooperation in legal matters.

B. Electronic Evidence

Cybercrime prosecutions depend highly on electronic evidence. The locations of the crime may be established by IP address, details about devices used, transaction history, e-mail, metadata, CCTV footage, server logs, and information about mobile devices.

The BSA recognizes electronic and digital evidence in the text of law. (BSA) Section 61 stipulates that electronic or digital evidence shall not be assessed as inadmissible just because it is of electronic form, but it is subject to section 63. Sections 62 and 63 outline the evidential provisions about electronic evidence.[13]

Although having statutory recognition is good, it doesn't solve numerous problems connected with electronic evidence being admissible. Evidence must be preserved, authenticated, and directly related to a defendant. Investigative difficulties may arise due to the encryption of information, deletion, the use of the cloud, the use of many devices, and information being in the hands of third parties.

The difference between a digital trace and attribution is crucial in this context. An IP address, a device, and an account may be used in investigation as evidence. However, they cannot prove responsibility on their own. Cybercrime investigation requires combining technical evidence with circumstances of the case, as well as using traditional investigation methods.

13. Bharatiya Sakshya Adhiniyam, No. 47 of 2023, §§ 61–63.

V. JUDICIAL DEVELOPMENT

Indian courts have been instrumental in establishing the limits of constitutional law and admissibility of evidence in cyber law.

A. *Shreya Singhal v. Union of India*

The Supreme Court of India declared unconstitutional section 66A of the Information Technology Act, which limited free speech protected by the Constitution.[14] This ruling indicates that the field of cyber law falls under the purview of constitutional law. Therefore, criminal law which concerns with online expression cannot be vague and general.

The ruling is also important because attempts to regulate so-called harmful behaviour online might obstruct legitimate speech. Therefore, any efficient legislation on cyber crime must distinguish between criminal acts and expression which some people may find offensive or annoying.

B. *Anvar P.V. v. P.K. Basheer*

In the case of *Anvar P.V. vs. P.K. Basheer,* the Supreme Court pointed out the relevant statutory provisions on admissibility of electronic evidence under the Indian Evidence Act.[15] The ruling illustrated the pivotal aspect of commencing prosecution of cyber fraud: the mere possession of electronic evidence does not render it admissible in court.

14. *Shreya Singhal v. Union of India,* (2015) 5 SCC 1 (India).
15. *Anvar P.V. v. P.K. Basheer,* (2014) 10 SCC 473 (India).

C. *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*

Moreover, in the case of *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal,* the Court again stressed the importance of adhering to the regulations applicable to electronic evidence. [16] While the BSA has replaced the Indian Evidence Act, the conclusions drawn here remain applicable: digital evidence should be subject to due process requirements.

The problem is aggravated as nowadays evidence can be maintained by telecom companies, banks and financial institutions, cloud-service providers or foreign IT companies, thus requiring effective prosecution to go beyond applicable laws and establish timely access to such data.

D. *Justice K.S. Puttaswamy v. Union of India*

J*ustice K.S. Puttaswamy (Retd.) v. Union of India* has added to the constitutional aspect of cyber regulation as the Supreme Court has ruled that privacy is a fundamental right protected under the constitution.[17] Cyber-crime investigations require the collection of personal data such as messages, location information, content of devices, and financial records. Therefore, the State has the obligation to investigate crimes while also weighing the need to protect the citizens' privacy from excessive intrusion.

VI. Limitations of India's Existing Remedies

Even though there are plenty of statutes, the enforcement of laws cannot be guaranteed.

First, the law in India is highly fragmented. The existing protection systems include multiple laws, namely, the IT Act, BNS, BNSS, BSA and DPDP Act, covering various areas; law regarding cybersecurity also includes executive measures and sector-specific approaches. While this fragmentation does not present an inherent flaw, lack of coordination between those systems may create certain difficulties for investigators and victims.

16. *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal,* (2020) 7 SCC 1 (India).
17. *Justice K.S. Puttaswamy (Retd.) v. Union of India,* (2017) 10 SCC 1 (India).

Second, the issue of attribution remains the biggest challenge from the technical perspective. Cybercriminals can exploit stolen logins and passwords, utilize virtual private networks, work through compromised computers, whereby it is much easier to track the device than to prove who actually controlled it at the relevant time.

Third, cybercrime is often transnational in nature. An Indian victim could potentially interact with a foreign online portal, maneuver through various bank accounts and make transactions between the offender and themselves situated outside Indian territory. Traditional investigative methods are thus often outpaced by the speed of disappearance or movement of electronic evidence.

Fourth, cases of under-reporting make legal remedies less effective. Victims tend to shy away from reporting fraud due to reasons like shame, fear of getting stigmatized or the feeling of not knowing who to turn to.

Moreover, investigations of cybercrimes necessitate a certain level of institutional capacity. Investigators need to be well versed in issues of digital forensic science, viruses, transactions made via cryptocurrency, extraction devices, cloud technology, as well as preservation of electronic evidence.

In light of the above arguments, it can be stated that cybercrime related issues in India are more related to enforcement issues as opposed to mere legislative ones.

VII. Towards a more Effective Framework

It is essential to begin any future reforms with the recognition that another all-encompassing cybercrime law is not necessarily the solution. Rather, introducing an additional law may lead to more disintegration of the existing legal framework.

The key part here is that institutions need to coordinate their work. Police cybercrime units, ordinary police officers, prosecutors, forensic labs, and specialized cybersecurity institutions

must find ways to exchange their knowledge and evidence. Cybercrime should not be recognized as an exclusive concern of specialized agencies, given that many crimes can be handled by ordinary police.

Furthermore, in order to increase investigative capacities the institutions must continuously invest in training. Training must go beyond mere knowledge of what cybercrime is to include digital forensics, tracking cryptocurrencies, digital evidence in the cloud, malware analysis, and archiving electronic records.

Thirdly, it is of utmost importance that the legal system assumes speed in determining financial cybercrime cases in view of the fact that virtual money can move between various bank accounts in a matter of minutes. As a result, the recovery of the stolen funds may not be very useful for the victims.

Fourth, one must ensure that electronic evidence is preserved right after the initiation of the investigation. The procedural framework should be implemented by the professionals who possess sufficient knowledge in terms of defining any relevant type of evidence and preserving them before it is deleted, modified or sent outside of the jurisdiction.

Finally, one needs to make sure that the police work within constitutional limits. Cybersecurity should not be used as an excuse for unlimited surveillance or unspecific regulations in the internet. The experience from the cases of Shreya Singhal and Puttaswamy shows that an efficient cybercrime system should protect not only the interests of the society but also personal freedoms.

VIII. Conclusion

In the conclusion, it is highlighted that India has made some strides in the development of its legal framework in relation to cybercrime. In regard to this, the IT Act still keeps on defining particular offences of this kind. The BNSS also aims to tackle cases of any cyber-related crimes. The BNSS mentions the methods of electronic communications, and the BSA makes it possible to define rules for the use of different kinds of evidence in cyberspace. The DPDP Act also

created a separate legal framework for personal data protection in cyberspace. Moreover, the announcement of the DPDP Rules of 2025 is another milestone for the development of the country's data protection regime.[18]

In spite of the abundance of legal acts regulated by the authorities of India in regard to cybercrime, this fact should not be confused with effectiveness. The nature of cybercrime makes it technologically complex.

The major problem for India today is not only the problem of distinguishing new forms of cyber offences. India needs to ensure that there are effective ways to provide remedies for the people. For this purpose, it is imperative to combine substantive laws with procedural laws, laws of evidence, and cybersecurity laws and data privacy laws with the principles of constitutional law.

Therefore, India should focus on improving the practical aspects of the law rather than on introducing new crimes into its legislative framework. Thus, the success of cyber laws should be determined by the ability of victims to make use of effective remedies for their problems rather than the number of laws constituting the basis for cyber legislation.

18. Ministry of Electronics & Information Technology, Digital Personal Data Protection Rules, 2025 (Nov. 14, 2025).