Original Article
ISSN(Online): 3139-6747
https://thevisionaryspectrum.com/

THE VISIONARY SPECTRUM
JOURNAL OF INNOVATION AND INTERDISCIPLINARY RESEARCH
Volume 01, Issue 02, June 2026

Cyber Crimes and Challenges under the Bharatiya Nyaya Sanhita

Dr. Ajay Vikram Singh
Assistant Professor, Govt. PG Law College, Sikar, Rajasthan
Email: vkrmajaysingh@gmail.com

Abstract:

The rapid expansion of digital payments, social media, cloud computing and artificial intelligence has increased both the scale and complexity of cybercrime in India. Online financial fraud, identity theft, cyberstalking, intimate-image abuse, electronic forgery, organised cybercrime and synthetic-media manipulation now affect individuals, businesses and public institutions. This article examines the treatment of cybercrime under the Bharatiya Nyaya Sanhita, 2023, and its relationship with the Information Technology Act, 2000. It follows a qualitative and doctrinal methodology based on legislation, rules, official crime statistics and the new procedural and evidentiary laws. The Sanhita recognises electronic and digital records, includes cybercrime within organised crime and applies conventional offences such as cheating, personation, forgery, intimidation and stalking to technology-enabled conduct. Nevertheless, core computer offences remain governed by the Information Technology Act. The study identifies challenges relating to statutory overlap, artificial-intelligence-generated deception, cross-border investigation, attribution, electronic evidence, investigative capacity and victim redressal. It recommends clearer charging guidelines, technology-neutral definitions, specialised investigation, stronger forensic capacity and coordinated platform and banking responses.

Keywords: Cybercrime, Bharatiya Nyaya Sanhita, information technology law, online fraud, electronic evidence, organised cybercrime.

Received 02 June 2026
Accepted 10 June 2026
Published 20 June 2026

Corresponding Author:
Dr. Ajay Vikram Singh
Email: vkrmajaysingh@gmail.com

Doi:https://doi.org/10.64880/tvsjiir.v1i2.01

Funding: This research received no specifics grant from any funding agency in the public, commercial, or not-for-profit sector.

1. Introduction

Digital technology has transformed Indian social and economic life. Banking, government services, education, commerce, healthcare and personal communication now depend extensively upon internet-enabled devices and digital platforms. These systems offer speed and convenience, but they

also create opportunities for fraud, unauthorised access, impersonation, surveillance and large-scale exploitation. A criminal may now deceive thousands of victims without being physically present in the same city or even the same country.

Cybercrime is not a single offence. It includes crimes in which a computer system or network is the target, such as hacking, malware attacks and denial-of-service activity. It also includes conventional offences committed through digital means, such as cheating, extortion, stalking, forgery, intimidation and sexual exploitation. In a third category, technology both enables and intensifies the offence by making content permanent, searchable, reproducible and capable of immediate global circulation.

The National Crime Records Bureau recorded 101,928 cybercrime cases across India in 2024, compared with 86,420 in 2023 and 65,893 in 2022. The 2024 total included 29,758 fraud cases, 19,296 cheating cases, 1,240 cases of cyberstalking or cyberbullying involving women and children, 702 forgery cases, 601 cyber-blackmail or threatening cases and 60 organised cybercrime cases. Registered cases represent police records rather than the actual prevalence of victimisation, since many offences remain unreported or are classified under different legal provisions.

The Bharatiya Nyaya Sanhita, 2023—hereafter referred to as the BNS—came into force on 1 July 2024 and replaced the Indian Penal Code, 1860. It consolidates general criminal offences, but it does not replace the Information Technology Act, 2000. Cybercrime in India is therefore governed through a combined framework in which the BNS addresses general and technology-enabled criminal conduct, while the Information Technology Act deals specifically with unauthorised computer activity, identity theft, privacy violations, obscene electronic content and cyberterrorism.

2. Objectives of the Study

The principal objectives of this article are:

1. To explain the nature and classification of cybercrime in contemporary India.
2. To examine the provisions of the BNS applicable to cyber-enabled offences.
3. To analyse the relationship between the BNS and the Information Technology Act.
4. To study procedural and evidentiary developments under the new criminal laws.
5. To identify major challenges in investigation, prosecution and victim protection.
6. To suggest reforms for a coherent and technology-responsive cybercrime framework.

3. Research Methodology

The study follows a qualitative, doctrinal and analytical research method. Primary sources include the Bharatiya Nyaya Sanhita, 2023; the Information Technology Act, 2000; the Bharatiya Nagarik Suraksha Sanhita, 2023; the Bharatiya Sakshya Adhiniyam, 2023; and the Information Technology Rules updated through 2026.

Official statistics and institutional information have been drawn from the Ministry of Home Affairs, the National Crime Records Bureau, the Indian Cyber Crime Coordination Centre and the National Cyber Crime Reporting Portal. No primary survey or experimental study has been undertaken. The numerical information reproduced in the article is drawn only from official government sources.

4. Concept and Classification of Cybercrime

Cybercrime may be understood as unlawful conduct in which digital technology functions as a target, instrument, environment or source of evidence. This broad definition is necessary because modern offences frequently combine several forms of conduct.

Computer-dependent crimes cannot ordinarily be committed without a computer system. These include unauthorised access, introduction of malware, disruption of networks, tampering with computer source code and attacks against protected systems.

Computer-enabled crimes are conventional offences whose reach is expanded through technology. Phishing, online investment fraud, matrimonial fraud, impersonation, cyberstalking, extortion and circulation of forged electronic records fall within this category.

Content-related offences involve the creation, transmission or publication of unlawful electronic content. Examples include child sexual abuse material, non-consensual intimate imagery, sexually explicit content, threatening messages and unlawful synthetic media.

Cyber-economic and organised crimes involve structured networks, mule bank accounts, fraudulent call centres, cryptocurrency transfers, mass-marketing schemes, malicious applications and coordinated attacks. These offences often cross state and national boundaries and involve specialised division of labour.

The legal classification is important because no single provision applies to every cybercrime. A fraudulent message may simultaneously involve identity theft under the Information Technology Act, cheating by personation under the BNS, electronic forgery and criminal conspiracy. Investigating agencies must therefore identify the conduct, intention, computer-related act and resulting harm separately.

5. Digital Recognition under the Bharatiya Nyaya Sanhita

One significant feature of the BNS is its express recognition of electronic and digital records. Section 2 defines a “document” to include an electronic or digital record intended to be used, or capable of being used, as evidence of a matter. This definition ensures that emails, electronic contracts, digitally transmitted records, online certificates and similar materials can fall within offences concerning false documents and forgery.

The recognition does not create a complete code of computer offences. Rather, it modernises conventional criminal-law concepts so that offences involving documents, deception and evidence can operate in a digital environment. The nature of the offence continues to depend upon dishonesty, fraud, intention, knowledge and the harm produced.

This approach is useful because technology changes more rapidly than individual criminal techniques. A law framed only around one form of communication may quickly become obsolete. At the same time, broad language must be applied carefully so that ordinary errors, parody, editing and lawful digital activity are not treated as forgery or fraud without proof of the required criminal intention.

6. Organised Cybercrime under Section 111

Section 111 represents the most direct recognition of cybercrime in the BNS. It includes cybercrime within the activities that may constitute organised crime when committed as a continuing unlawful

activity by a person or group acting as part of, or on behalf of, an organised crime syndicate to obtain direct or indirect material benefit.

The provision is relevant to organised phishing networks, fraudulent call centres, ransomware groups, large-scale investment scams, credential-selling networks and coordinated digital extortion. It also covers participation, facilitation, conspiracy, preparatory activity, membership of an organised crime syndicate and harbouring certain offenders. Where organised crime does not result in death, the punishment may range from a minimum of five years to imprisonment for life, along with a minimum fine of five lakh rupees.

However, not every repeated cyber offence automatically becomes organised crime. The statutory definition of "continuing unlawful activity" requires a cognisable offence punishable with imprisonment of three years or more and more than one charge-sheet filed before a competent court during the preceding ten years, with the court having taken cognisance. This threshold may help distinguish organised criminal enterprises from isolated misconduct, but it can also delay application against newly discovered syndicates whose earlier members or cases have not been formally linked.

The expression "cyber-crimes" is not separately defined in the BNS. Investigators and courts must therefore determine its scope by reading the provision with the Information Technology Act and the underlying criminal activity. Clear operational guidelines are needed to prevent inconsistent application across states.

7. Online Cheating and Personation

Online financial fraud commonly begins with deception. Offenders may impersonate bank officials, police officers, employers, relatives, traders or customer-support representatives. They may use fake websites, QR codes, mobile applications, investment groups or manipulated caller identities to induce a victim to transfer money or disclose credentials.

Section 318 of the BNS defines cheating as deceiving a person and fraudulently or dishonestly inducing that person to deliver property, allow property to be retained, or do or omit something that causes or is likely to cause harm in body, mind, reputation or property. Where the deception dishonestly induces delivery of property or alteration or destruction of a valuable security, the punishment may extend to seven years and fine.

Section 319 addresses cheating by personation. It applies where an offender pretends to be another person, knowingly substitutes one person for another or falsely represents that a person possesses another identity. The person impersonated may be real or imaginary. This provision is particularly relevant to fake profiles, executive impersonation, fraudulent customer-care accounts and AI-assisted voice impersonation.

These BNS provisions may operate together with section 66D of the Information Technology Act, which specifically punishes cheating by personation through a computer resource or communication device. Section 66C separately punishes fraudulent or dishonest use of another person's password, electronic signature or unique identification feature.

The overlap is legally understandable because one provision protects against deception and property harm, while the other focuses on misuse of computer resources and digital identity. Nevertheless, inconsistent charging practices can create confusion. Investigating officers require standard guidance explaining when both provisions should be invoked and how the different ingredients must be proved.

8. Electronic Forgery and Manipulated Records

Digital fraud frequently depends upon false invoices, forged certificates, altered screenshots, fabricated appointment letters, counterfeit identities and manipulated payment records. Sections 335 to 340 of the BNS expressly incorporate electronic records within offences concerning false documents and forgery.

Section 335 treats a person as making a false electronic record where the person dishonestly or fraudulently creates, transmits, electronically signs or materially alters a record with the intention that it be believed to have been made or authorised by another person. Section 336 defines forgery and imposes enhanced punishment where the forged document or electronic record is intended for cheating or harming reputation.

Section 337 applies to forged court records, public registers and government-issued identity documents, including Aadhaar and voter identity records. The provision expressly states that an electronic register includes lists, data or records maintained electronically. Section 340 punishes the fraudulent or dishonest use of a forged electronic record as genuine.

These provisions are capable of addressing many forms of digitally fabricated evidence and credentials. Artificial intelligence, however, introduces new questions. A synthetic voice, image or video may falsely represent a person without necessarily appearing in the traditional form of a signed document. Liability may depend upon whether the content qualifies as an electronic record, whether it was created with fraudulent intention and how it was used.

The Information Technology Rules updated in February 2026 now regulate synthetically generated information and require covered intermediaries to adopt measures concerning labelling, user declarations and provenance. These platform duties assist identification and moderation but do not by themselves create a comprehensive substantive criminal offence for every harmful deepfake.

9. Cyberstalking, Privacy and Sexual Offences

Section 78 of the BNS recognises cyberstalking by including the monitoring of a woman's use of the internet, email or another form of electronic communication. Repeated attempts by a man to contact a woman despite a clear indication of disinterest also constitute stalking, subject to limited statutory exceptions. A first conviction may attract imprisonment up to three years, while a subsequent conviction may attract imprisonment up to five years.

Section 77 addresses voyeurism and expressly covers dissemination of an image where a woman consented to its capture but did not consent to distribution to third persons. Section 75 may apply to showing pornography against a woman's will or making sexually coloured remarks. These provisions can operate alongside sections 66E, 67, 67A and 67B of the Information Technology Act,

which address electronic privacy violations, obscene material, sexually explicit material and content involving children.

The combined framework provides important protection but remains fragmented. Synthetic nudity, face-swapped sexual content, cyber flashing and threats to distribute intimate material may require several provisions depending upon the facts. Some BNS provisions are also gender-specific, while online offences may be committed anonymously, collectively or through automated systems.

A consent-centred and technology-neutral offence of image-based sexual abuse would provide greater clarity. Such an offence should distinguish consent to create or privately share an image from consent to public distribution and should cover genuine, altered and entirely synthetic intimate content.

10. Threats, Blackmail and Harmful Electronic Communication

Digital communication is commonly used for threats involving violence, reputation, private images or financial loss. Section 351 of the BNS defines criminal intimidation broadly as threatening another "by any means" with injury to person, reputation or property with the intention of causing alarm or compelling conduct. Anonymous communications or deliberate concealment of the sender's identity may attract additional punishment.

This provision is relevant to threatening emails, anonymous social-media messages, sextortion and ransomware demands. Depending upon the facts, extortion provisions may also apply where the threat is used to obtain money, property, credentials or another benefit.

Section 353 addresses false information, rumours and reports, including those circulated electronically, where the required intention or likelihood of causing specified public harm is established. The provision must be interpreted narrowly because criminal law should not punish mere inaccuracy, criticism or unpopular opinion without proof of statutory harm and mental intention.

This constitutional caution is particularly important because section 66A of the Information Technology Act, which criminalised broadly defined offensive online messages, was struck down by the Supreme Court in *Shreya Singhal v. Union of India*. The updated official text of the Information Technology Act records the invalidation of section 66A.

11. Continuing Role of the Information Technology Act

The BNS does not contain technical offences corresponding to every form of cyber misconduct. The Information Technology Act remains the principal special law for computer-related offences.

Section 65 punishes tampering with computer source documents. Section 66 applies where acts specified under section 43—such as unauthorised access, downloading, copying, introducing contaminants, damaging systems or disrupting access—are committed dishonestly or fraudulently. Sections 66B to 66E address receipt of stolen computer resources, identity theft, computer-enabled personation and privacy violations. Section 66F deals with cyberterrorism. Sections 67 to 67B regulate unlawful electronic sexual and obscene content, while section 67C concerns preservation and retention of information by intermediaries.

The two statutes should therefore be understood as complementary. The Information Technology Act identifies the technical computer-related conduct, while the BNS addresses the wider deception, intimidation, conspiracy, organised activity, forgery or harm. Section 77 of the Information Technology Act expressly indicates that compensation, penalties or confiscation under that Act do not interfere with punishment under another law.

A practical problem arises when the same conduct satisfies multiple offences carrying different classifications, punishments and evidentiary requirements. Prosecutors must avoid both undercharging and unnecessary multiplication of charges. A nationally applicable charging protocol could improve consistency.

12. Procedure, Reporting and Electronic Evidence

The Bharatiya Nagarik Suraksha Sanhita permits information concerning a cognisable offence to be given orally or through electronic communication to the officer in charge of a police station, irrespective of where the offence occurred. Where information is supplied electronically, it must be signed by the informant within three days. This provision can assist cybercrime victims who are uncertain about territorial jurisdiction. (India Code)

Victims may also file complaints through the National Cyber Crime Reporting Portal. The portal gives special attention to offences involving women and children, while immediate cyber-financial fraud may be reported through the 24-hour national helpline number 1930. Rapid reporting is important because early communication with banks and payment intermediaries can improve the possibility of freezing or restoring transferred funds. (Cyber Crime Portal)

The Bharatiya Sakshya Adhiniyam recognises electronic and digital records as admissible evidence and provides that they possess the same legal effect, validity and enforceability as other documents, subject to the statutory conditions governing electronic records. (India Code)

In practice, admissibility is only one part of the problem. Investigators must establish authenticity, integrity, source, time, device linkage and chain of custody. Screenshots may be incomplete or manipulated. Messages may be deleted, accounts may be compromised and metadata may be held by foreign companies. Proper forensic imaging, preservation requests, hash values, server logs and legally compliant certification remain essential.

13. Major Challenges

13.1 Statutory overlap and classification

The coexistence of the BNS and Information Technology Act creates comprehensive coverage but also produces overlapping offences. A phishing case may involve computer-enabled personation, cheating, identity theft, forgery and conspiracy. Different police units may apply different combinations of sections to similar conduct.

13.2 Cross-border jurisdiction

Cybercriminals can operate through foreign servers, virtual private networks, encrypted applications, cryptocurrency and stolen identities. The victim, offender, bank, intermediary and server may all be located in different jurisdictions. Obtaining subscriber data or content from another country may involve lengthy legal-assistance procedures.

13.3 Attribution and anonymity

An internet-protocol address does not necessarily identify the person who committed the offence. Devices may be shared, compromised or remotely controlled. Criminal groups use mule accounts, forged subscriber details and layered transfers. Establishing attribution requires technical, financial and circumstantial evidence rather than reliance upon one digital identifier.

13.4 Artificial intelligence and deepfakes

AI tools can produce convincing voice clones, forged video calls and fabricated documents at low cost. Existing cheating and forgery provisions may apply, but identifying the creator, proving manipulation and distinguishing fraudulent content from satire or lawful creative work remain difficult.

13.5 Investigative and forensic capacity

The Ministry of Home Affairs reported that cyber forensic-cum-training laboratories had been commissioned in 33 states and Union Territories and that more than 24,600 law-enforcement personnel, prosecutors and judicial officers had received relevant training. Seven Central and 28 State Forensic Science Laboratories were operational, while the National Digital Investigation Support Centre had assisted in more than 14,064 cybercrime cases by 30 June 2026. Despite this expansion, the growth and technical complexity of cybercrime continue to place considerable pressure on institutional capacity. (Press Information Bureau)

13.6 Underreporting and victim awareness

Victims may delay reporting because of embarrassment, uncertainty, small initial financial loss or lack of knowledge about evidence preservation. Delay may allow money to pass through multiple accounts and digital content to spread further. Awareness must therefore include practical instructions about reporting, password changes, account preservation and communication with banks.

13.7 Balancing security and civil liberties

Cybercrime regulation can affect privacy, anonymity, encryption and freedom of expression. Excessively broad offences or unrestricted surveillance may weaken constitutional rights. Investigative powers should therefore operate under clear legal authority, necessity, proportionality and effective oversight.

14. Findings and Recommendations

The study finds that the BNS has strengthened the general criminal-law response to cybercrime by recognising electronic records, incorporating organised cybercrime and extending offences such as stalking, cheating, forgery and intimidation to digital conduct.

However, the BNS is not a self-contained cybercrime law. The Information Technology Act remains essential for defining unauthorised access, system interference, identity theft, cyberterrorism and unlawful electronic content. Effective prosecution depends upon coordinated use of both statutes.

The following reforms are recommended:

1. **Uniform charging guidelines** should clarify the relationship between BNS and Information Technology Act provisions.

2. **Cybercrime terminology** under section 111 should be defined through statutory guidance, especially for organised digital fraud networks.
3. **Technology-neutral offences** should address harmful deepfakes, synthetic impersonation and image-based sexual abuse.
4. **Specialised cyber investigators and prosecutors** should be available at district and state levels.
5. **Electronic-evidence protocols** should standardise preservation, forensic imaging, chain of custody and certification.
6. **Banking and platform coordination** should enable immediate freezing, takedown and preservation requests.
7. **Cross-border cooperation** should be improved through faster lawful data-sharing mechanisms.
8. **Victim-centred remedies** should include rapid fund restoration, protection of intimate information, counselling and accessible complaint tracking.
9. **Periodic statutory review** should be conducted because cybercriminal techniques evolve more rapidly than conventional legislative cycles.

15. Conclusion

The Bharatiya Nyaya Sanhita marks an important stage in the modernisation of Indian criminal law. Its recognition of electronic records, organised cybercrime, electronic stalking, digital personation and electronic forgery allows traditional criminal-law principles to respond to several contemporary offences.

Nevertheless, cybercrime cannot be controlled through the BNS alone. The Information Technology Act continues to provide the specialised foundation for computer-related offences, while the Bharatiya Nagarik Suraksha Sanhita and Bharatiya Sakshya Adhiniyam regulate electronic reporting, investigation and evidence.

The principal challenge is no longer merely the absence of legal provisions. It is the need to apply overlapping laws consistently, preserve volatile evidence, identify anonymous offenders, obtain cross-border data and respond before money or harmful content becomes impossible to recover.

A credible cybercrime framework must be technologically informed, institutionally coordinated and constitutionally restrained. Strong enforcement is necessary, but it must be accompanied by clear definitions, procedural safeguards, specialised expertise and accessible remedies. Only such an integrated approach can ensure that criminal law remains effective as digital technologies and methods of deception continue to evolve.

References

Bharatiya Nagarik Suraksha Sanhita, 2023, Act No. 46 of 2023.

Bharatiya Nyaya Sanhita, 2023, Act No. 45 of 2023.

Bharatiya Sakshya Adhiniyam, 2023, Act No. 47 of 2023.

Government of India, Ministry of Electronics and Information Technology. (2026). *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, updated through 2026*.

Government of India, Ministry of Home Affairs. (2026). *National Cyber Crime Data: Crime in India 2024*.

Information Technology Act, 2000, Act No. 21 of 2000.

Shreya Singhal v. Union of India, (2015) 5 SCC 1.