ILE MULTIDISCIPLINARY JOURNAL [IF SCORE – 7.58]

VOLUME 4 AND ISSUE 2 OF 2025

APIS – 3920 – 0007 | ISSN - 2583-7230

Published by

Institute of Legal Education

https://iledu.in

CYBER CRIMES IN THE DIGITAL AGE: A STUDY UNDER BHARATIYA NYAYA SANHITA 2023[611]

AUTHOR - SNEHA RAVAL, STUDENT AT SLRTCL (MUMBAI UNIVERSITY)

BEST CITATION - SNEHA RAVAL, CYBER CRIMES IN THE DIGITAL AGE: A STUDY UNDER BHARATIYA NYAYA SANHITA 2023, ILE MULTIDISCIPLINARY JOURNAL, 4 (2) OF 2025, PG. 418-422, APIS – 3920-0007 | ISSN - 2583-7230.

Abstract

The rapid spread of digital technology has brought many conveniences, but it has also created space for new kinds of criminality — from phishing and identity theft to online stalking and deepfakes. The Indian Penal Code of 1860 was not designed for the digital era, and enforcement often relied on a mix of the IPC and the Information Technology Act, 2000. The Bharatiya Nyaya Sanhita, 2023 (BNS) tries to bring modern offences into the main criminal law by recognising electronic records and incorporating cyber-related conduct into existing and new offences. This paper examines how BNS addresses cyber-crimes, focussing on the provisions that explicitly or implicitly cover electronic wrongdoing (for example, definitions that include electronic records and sections on stalking, forgery of electronic records, organized crime involving cyber-offences, false information, and defamation).

Keywords- Cybercrime, Crime, Cyber Criminals, BNS, Technology.

[611]Bhartiya nyaya sanhita,2023 - Indian penal code,1860

ILE MULTIDISCIPLINARY JOURNAL [IF SCORE – 7.58]
VOLUME 4 AND ISSUE 2 OF 2025
APIS – 3920 – 0007 | ISSN - 2583-7230
Published by
Institute of Legal Education
https://iledu.in

Introduction –

Almost every person in urban India uses the internet for banking, communication, shopping, or entertainment. As our lives move online, criminals have followed. Modern offenders exploit anonymity, speed, and cross-border reach: fake social media profiles to defame and impersonate; OTP and phishing scams to steal money; hacking to access private data; and manipulated audio or video (deepfakes) to threaten reputations or influence public opinion.

The IPC (1860) was framed in a pre-digital age; it did not directly address electronic records or online modalities. For two decades, investigators and courts used the Information Technology Act, 2000, alongside the IPC to address cyber incidents — a pragmatic but sometimes messy arrangement. Investigations often required technical expertise and clarity about jurisdiction, evidence, and the nature of electronic documents.

After understanding how cyber law has developed in India so far, it is now important to see what changes the Bharatiya Nyaya Sanhita, 2023 brings. The next section looks at the specific provisions that cover cyber crimes."

The aim of this article is to analyse the approaches given in BNS and also about the introduction of the new provisions in Bhartiya Nyaya Sanhita 2023 helps in fighting these cybercriminals and particularly focusses to cope with these issues which are a threat to the society.

Background: evolution of cyber law in India-

India's legal response to cyber problems developed in stages. The IT Act, 2000 was the first specialised law for electronic records, digital signatures, and limited cyber offences (like hacking, unauthorised access, and certain online frauds). Over time, courts and police regularly combined IT Act provisions with IPC offences such as cheating, criminal breach of trust, defamation, or obscenity to prosecute digital wrongdoing.

Problems with that arrangement included:

1. **Overlap and uncertainty:** it was often unclear whether an act should be charged under the IPC, the IT Act, or both. This sometimes led to procedural confusion and duplicated investigations.
2. **Evidence and admissibility: c**ourts required clear rules and technical processes for electronic evidence (an area that improved but still demands technical skills)
3. **Jurisdictional issues:** the internet is borderless; tracing offenders and deciding where to try them remained a challenge.
4. **New technologies:** AI-generated content and complex financial cyberfraud outpaced both statutes and investigator expertise.

Against this background, BNS sets out to fold many cyber-relevant concepts directly into the criminal code. Rather than rely solely on a companion statute (the IT Act), BNS updates core criminal categories so that electronic means are explicitly within scope. This approach aims to reduce fragmentation and emphasise that crimes conducted by electronic means are as serious as their offline counterparts.

After understanding how cyber law has developed in India so far, it is now important to see what changes the Bharatiya Nyaya Sanhita, 2023 brings. The next section looks at the specific provisions that cover cyber crimes.

How Bharatiya Nyaya Sanhita, 2023 Deals with Cyber Crimes:-

The Bharatiya Nyaya Sanhita, 2023 (BNS) takes a different approach to cyber offences compared to earlier laws. Instead of creating a separate chapter for "cyber crimes," it directly includes electronic records and online conduct in many existing offences. This shows that crimes committed on the internet are to be treated as seriously as crimes in the physical world. Below are the most important provisions:

1. Section 78 – Stalking

- BNS broadens the meaning of stalking. It now clearly says that stalking is not only following someone physically but also using the

internet, email, or other electronic communication to harass them.

- Example: sending repeated WhatsApp messages even after being told to stop, or tracking someone's social media posts.

2. Section 111 – Organised Crimes

- Cyber crimes are often carried out by groups — for example, phishing gangs or online loan scams. BNS recognises this by including cyber offences within the definition of organised crime. This means stronger punishments and more powers for police to break these networks.
- Example: a call-centre scam cheating thousands of people across India.

3. Section 318 – Cheating by Personation using Computer Resources

- Under IPC, cheating by pretending to be someone was already a crime, but the law did not mention online methods. BNS makes it clear that cheating done through computer resources also counts.
- Example: creating a fake bank email asking for OTPs or setting up a fake social media account to trick people.

4. Section 336 – Forgery of Electronic Records

- Earlier, forgery meant faking a paper document. Today, it is easy to fake a PDF, Aadhaar card scan, or salary slip. BNS now includes electronic records in the definition of forgery.
- Example: editing a digital payslip to get a loan from a bank.

5. Section 353 – False Information and Deepfakes

- BNS recognises the harm caused by false digital content. It punishes spreading misinformation or creating manipulated material like deepfake videos if they can cause fear, hatred, or harm to public order.
- Example: circulating a fake video of a leader to mislead the public.

6. Section 356 – Defamation via Electronic

- Defamation is not new, but BNS clarifies that it also covers online platforms like emails, WhatsApp, and social media. Example: posting lies about a colleague on Facebook or sending a defamatory group email.
- Section 1(5)© – Jurisdiction in Cyber Crimes
- Since the internet has no borders, BNS says that Indian law applies even if the crime happens outside India, as long as the computer system targeted is located in India.
- Example: a hacker in another country stealing data from an Indian bank

7. Sections 66–70 – Cyber Offences and Digital Evidence:

- Cover unauthorized access to computer systems, online fraud, publication of harmful content, network misuse, and preservation of electronic records. These provisions strengthen the enforcement of cyber crime laws and ensure that offences like hacking, impersonation, and online defamation are properly addressed
- These provisions show that BNS accepts the reality of the digital age. Instead of leaving online offences only to the IT Act, it makes them part of India's main criminal law.

8. Comparision of IPC and BNS in Cyber Crimes

The table below shows how the Indian Penal Code (IPC), 1860, and the Bharatiya Nyaya Sanhita (BNS), 2023, handle different cyber offences. It highlights what is new or improved in the BNS.

Online Cheating:

IPC: Section 420 – Cheating (general, not specific to online).

BNS: Section 318 – Cheating using computer resources.

What's New: Online scams and impersonation are now clearly punishable.

Cyber Stalking:

IPC: No clear law.

BNS: Section 78 – Cyber Stalking.

What's New: Harassment or stalking via social media, emails, and messages is a crime.

Forgery of Electronic Records:

IPC: Sections 463–464 – Forgery (only physical documents).

BNS: Section 336 – Forgery of Electronic Records.

What's New: Making fake or altered digital files is illegal.

Online Defamation:

IPC: Sections 499–500 – Defamation (general, not specific to online).

BNS: Section 356 – Defamation via Electronic Means.

What's New: Posting false or harmful content online, such as on social media, is punishable.

Deepfakes / False Digital Information:

IPC: Not addressed.

BNS: Section 353 – False Info & Deepfakes.

What's New: Creating fake videos or images using AI to mislead people is now a crime.

Organised Cyber Crime:

IPC: No specific law for groups/networks.

BNS: Section 111 – Organised Cyber Crime.

What's New: Groups committing cyber crimes can be punished, not just individuals.

Jurisdiction Issues:

IPC: Territorial laws; no clear rules for cross-border cyber crimes.

BNS: Section 1(5)© – Jurisdiction in Cyber Crimes.

What's New: Courts now have clear rules for cases that cross state or national borders.

9. Significance of BNS Provisions: Cyber Crime in the Digital Age:-

The Bharatiya Nyaya Sanhita (BNS), 2023, introduces several important changes for cyber crime law in India. Its significance can be understood under the following points:

1. **Recognition of Modern Cyber Threats**
   - **-**Cyber stalking, online impersonation, deepfakes, and organized cyber crimes are explicitly defined as offences.
   - Courts and law enforcement now have clear guidance on how to handle such cases.
2. **Jurisdictional Clarity**
   - **-**Section 1(5)© addresses where cases can be filed and prosecuted, especially for cross-border cyber offences.
   - -This resolves confusion that existed under IPC, making legal action faster and more effective.
3. **Technology-Friendly Legal Provisions**
   - **-**Electronic records, AI-generated content, and online harassment are recognized and protected under law.
   - -The law not only punishes offenders but also acts as a deterrent for potential cyber criminals.
4. **Societal Protection and Digital Accountability**
   - **-**BNS safeguards privacy, security, and personal dignity in digital spaces.
   - -It promotes awareness and responsible use of technology among citizens.
5. **Modernizing Criminal Law**
   - -BNS updates criminal law to match the digital era.
   - -It bridges the gap between traditional legal provisions and contemporary cyber threats.

8. Challenges and Limitations of BNS in Addressing Cyber Crimes-

While the Bharatiya Nyaya Sanhita (BNS), 2023, has modernized criminal law for the digital age, several challenges and limitations remain in its implementation:

1. **Rapidly Evolving Technology**

-Cyber crimes evolve faster than legislation.

-New technologies, tools, and platforms may create offences that current laws don't yet cover.

2. **Overlap with the IT Act, 2000**

-Some provisions of BNS overlap with the Information Technology Act, 2000.

-This can create confusion about which law should be applied in specific cases.

3. Lack of Trained Cyber Police and Experts

Effective enforcement requires skilled cyber investigators and digital forensic experts.

-Currently, there is a shortage of trained personnel to handle sophisticated cyber crimes.

4. Low Awareness Among Citizens

-Many victims are unaware of legal remedies available for cyber crimes.

-This reduces reporting and delays justice, limiting the effectiveness of BNS.

5. Privacy and Free Speech Concerns

-Some provisions may conflict with privacy rights or freedom of expression.

-Striking the right balance between security and civil liberties is still a challenge.

Findings and suggestions: -

The study of cyber crimes under the Bharatiya Nyaya Sanhita (BNS), 2023, reveals both progress and areas needing improvement.

Findings:

The Bharatiya Nyaya Sanhita (BNS), 2023 updates India's criminal law to clearly define cyber crimes like online cheating, stalking, fake digital records, and deepfakes. It makes it easier for police and courts to investigate and punish these crimes. Still, challenges remain, such as fast-changing technology, lack of trained cyber experts, and low awareness among people.

***Suggestion*: -**

- Align BNS with IT laws to avoid confusion.
- Train police and courts in handling cyber crimes.
- Raise public awareness about online safety.
- Update laws regularly for new technologies.
- Cooperate with other countries on cross-border cyber crimes.

***Conclusion*:**

The Bharatiya Nyaya Sanhita (BNS), 2023 brings India's criminal law in line with the needs of the digital age by clearly defining cyber crimes such as online cheating, stalking, deepfakes, and organized cyber offences. It fills the gaps left by the Indian Penal Code (IPC) and provides stronger legal tools and clearer jurisdiction for handling online crimes. Still, to be truly effective, the law must be supported by better training for cyber experts, regular updates to cover new technologies, and greater public awareness so that citizens can protect themselves and seek justice.

***References*:-**

1. The bharatiya nyaya Sanhita, 2023
2. The indian penal code, 1860
3. The information technology act,2000
4. https://advocategandhi.com/cyber-crime-under-the-bharatiya-nyaya-sanhita-a-new-era-of-digital-justice/
5. https://doonlawmentor.com/cybercrime-under-bharatiya-nyaya-sanhita-challenges
6. https://www.linkedin.com/pulse/bharatiya-nyay-sanhita-provisions-regarding-cyber-shintre-bhagwat-69fjf