International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2024: 7.101

Investigation of Cyber Crimes in India: Procedural Challenges Under the Bharatiya Nagarik Suraksha Sanhita, 2023

Vijay Kumar

Jannayak Karpoori Thakur Vidhi Mahavidyalaya, Buxar, Bihar, India
Email: *kumarvijay2409[at]gmail.com*

Abstract: ***The exponential growth of digital technology has resulted in a corresponding increase in cyber crimes, posing serious challenges to the criminal justice system in India. While substantive laws addressing cyber offences have evolved through the Information Technology Act, 2000 and the Bharatiya Nyaya Sanhita, 2023, effective investigation remains the most critical and complex aspect of cyber crime enforcement. The Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS), which replaces the Code of Criminal Procedure, 1973, introduces a renewed procedural framework governing criminal investigation, including cyber crime cases. This article undertakes a doctrinal and analytical study of the investigation of cyber crimes in India with specific focus on procedural challenges under the BNSS, 2023. It examines issues relating to jurisdiction, digital evidence, investigative powers of the police, and safeguards ensuring fair investigation. The article argues that although the BNSS provides a structured procedural mechanism, effective investigation of cyber crimes continues to face institutional, technical, and practical challenges. It concludes that successful implementation of the BNSS framework requires specialised training, technological infrastructure, and continuous judicial oversight to ensure justice in cyber crime cases.***

Keywords: Cyber Crime Investigation; BNSS 2023; Digital Evidence; Criminal Procedure; Fair Investigation

1. Introduction

Cyber crimes have emerged as one of the most serious threats to modern society. Offences such as online fraud, identity theft, hacking, cyber stalking, and data breaches have increased significantly with the expansion of digital platforms. Unlike conventional crimes, cyber offences are characterised by anonymity, speed, and transnational reach, making investigation particularly difficult.

In India, the legal framework addressing cyber crimes has developed primarily through substantive laws such as the Information Technology Act, 2000 and, more recently, the Bharatiya Nyaya Sanhita, 2023. However, the effectiveness of these laws largely depends on the procedural mechanisms governing investigation. The enactment of the Bharatiya Nagarik Suraksha Sanhita, 2023 marks a significant reform in criminal procedure by replacing the Code of Criminal Procedure, 1973. This article analyses how the BNSS addresses the investigation of cyber crimes and highlights the procedural challenges that continue to impede effective enforcement.

2. Nature of Cyber Crime Investigation

Cyber crime investigation differs fundamentally from traditional criminal investigation. Physical evidence is often absent, and the primary form of evidence is digital in nature. Electronic records, server logs, IP addresses, and digital trails form the backbone of cyber crime investigation.

Another defining feature of cyber crimes is their borderless nature. Offences may be committed in one jurisdiction, while victims, servers, and accused persons may be located in different states or even different countries. This creates complex issues relating to jurisdiction, coordination between agencies, and admissibility of evidence.

3. Investigation Powers Under the BNSS, 2023

The BNSS governs the procedural aspects of investigation, including cyber crime cases. While the Sanhita does not create separate procedures exclusively for cyber offences, its general investigative framework applies equally to digital crimes.

3.1 Registration of FIR

The investigation process begins with the registration of a First Information Report. In cyber crime cases, FIR registration often faces practical difficulties due to lack of clarity regarding territorial jurisdiction. The BNSS reinforces the duty of the police to register FIRs and initiate investigation, thereby addressing one of the major hurdles faced by cyber crime victims.

3.2 Powers of Investigation

The BNSS confers wide investigative powers on police officers, including the authority to collect evidence, examine witnesses, and conduct searches and seizures. In cyber crime cases, these powers extend to the collection of electronic evidence such as computers, mobile devices, and digital storage media. However, the effective exercise of these powers requires technical expertise, which is often lacking at the ground level.

3.3 Handling of Electronic Evidence

Electronic evidence plays a central role in cyber crime investigation. The BNSS recognises the importance of

proper procedure in collection and preservation of such evidence. Any lapse in procedure may compromise the integrity of digital evidence, thereby weakening the prosecution's case.

4. Procedural Challenges in Cyber Crime Investigation

Despite the procedural framework provided by the BNSS, several challenges continue to hamper effective investigation of cyber crimes.

4.1 Jurisdictional Issues

Cyber crimes frequently involve multiple jurisdictions. Determining the appropriate police station and court often becomes contentious, leading to delays and procedural confusion. Although the BNSS seeks to streamline procedural aspects, jurisdictional complexities remain a significant challenge.

4.2 Technical Expertise and Infrastructure

Effective cyber crime investigation requires specialised technical knowledge and advanced infrastructure. Many investigating officers lack adequate training in handling digital evidence, tracing cyber trails, and understanding complex technological processes. This gap significantly affects the quality of investigation.

4.3 Delay in Investigation

Cyber crimes demand swift action to preserve volatile digital evidence. Delays in investigation often result in loss or tampering of electronic data. Procedural delays, coupled with technical constraints, reduce the chances of successful prosecution.

4.4 Inter-State and International Cooperation

Cyber crimes often transcend state and national boundaries. Investigation in such cases requires coordination between multiple agencies and jurisdictions. Procedural limitations and lack of streamlined cooperation mechanisms further complicate the investigation process.

5. Safeguards Ensuring Fair Investigation

While empowering law enforcement agencies, the BNSS also incorporates safeguards to ensure fairness and prevent abuse of investigative powers.

5.1 Protection of Personal Liberty

Article 21 of the Constitution of India guarantees the right to personal liberty. Investigative procedures under the BNSS must conform to the constitutional mandate of fairness, reasonableness, and due process.

5.2 Procedural Accountability

The BNSS emphasises documentation and procedural compliance during investigation. Such requirements promote accountability and facilitate judicial scrutiny of investigative actions.

5.3 Rights of the Accused and Victims

A fair investigation protects not only the rights of the accused but also the interests of victims. In cyber crime cases, victims often face secondary victimisation due to procedural delays and lack of support. The procedural framework must therefore balance both interests.

6. Judicial Approach to Fair Investigation

The judiciary has consistently emphasised the importance of fair and impartial investigation as an essential component of criminal justice. The Supreme Court has held that investigation must be conducted in a manner that inspires confidence and adheres to constitutional principles.

In cyber crime cases, courts have underscored the need for proper handling of digital evidence and adherence to procedural safeguards. Judicial oversight thus acts as a crucial mechanism to ensure that investigative powers under the BNSS are not misused.

7. Way Forward

To address the procedural challenges in cyber crime investigation, several measures are necessary:

- Specialised Training: Investigating officers must receive regular training in cyber forensics and digital investigation techniques.
- Technological Infrastructure: Adequate infrastructure and forensic facilities must be established to support effective investigation.
- Inter-Agency Coordination: Mechanisms for cooperation between state, national, and international agencies must be strengthened.
- Judicial Sensitisation: Courts must remain vigilant to ensure procedural compliance and protection of fundamental rights.

8. Conclusion

The investigation of cyber crimes presents unique procedural challenges that cannot be addressed through conventional investigative methods alone. The Bharatiya Nagarik Suraksha Sanhita, 2023 provides a structured procedural framework governing criminal investigation, including cyber crime cases. While the Sanhita strengthens procedural accountability and reinforces safeguards ensuring fair investigation, significant challenges remain in its practical implementation. Effective investigation of cyber crimes under the BNSS requires not only statutory clarity but also technical expertise, institutional capacity, and continuous judicial oversight. A holistic approach that integrates legal reform with technological and administrative measures is essential to ensure justice in cyber crime cases.

References

[1] Bharatiya Nagarik Suraksha Sanhita, 2023

[2] Bharatiya Nyaya Sanhita, 2023
[3] Information Technology Act, 2000
[4] Constitution of India