International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

The Evolving Cybercrime Landscape in India: Legal Challenges, Digital Evidence, and New Criminal Laws

Mr. Saumya Deep Singh[1], Mr. Shirsh Pandey[2]

[1]LLM 2yr Student, Faculty of Juridical Sciences, Rama University
[2]Assistant Professor

Abstract
With the rapid expansion of digital technology, cybercrime has emerged as a significant legal challenge in India. The increasing instances of hacking, financial fraud, identity theft, cyber terrorism, and AI-driven offenses necessitate robust legal frameworks and efficient investigative mechanisms. The introduction of Bharatiya Nyaya Sanhita (BNS), 2023, Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023, and Bharatiya Sakshya Adhiniyam (BSA), 2023, marks a paradigm shift in India's criminal justice system, replacing colonial-era laws and adapting to the digital landscape. This paper examines the admissibility and investigation of digital evidence under these new laws, analyzing their significance, advantages, challenges, and implications for law enforcement, judiciary, and civil liberties. While these reforms streamline digital evidence collection and prosecution of cybercrimes, concerns persist regarding privacy violations, evidence tampering, jurisdictional issues, and forensic infrastructure gaps. The study suggests the need for specialized cyber forensic training, international cooperation, AI crime regulation, and improved cyber investigation infrastructure to ensure an effective and balanced legal regime.

Keywords: Cybercrime, Digital Evidence, Bharatiya Nyaya Sanhita, Bharatiya Nagarik Suraksha Sanhita, Bharatiya Sakshya Adhiniyam, Indian Criminal Laws, Cyber Forensics, AI Crimes, Privacy Protection, Digital Investigation, Legal Challenges.

1. Introduction

With rapid digitization, cybercrime has become one of the most pressing concerns in India. The rise of hacking, financial frauds, identity theft, cyber terrorism, and other digital offenses has necessitated robust legal frameworks. Digital evidence plays a critical role in cybercrime investigations, but its admissibility, authentication, and reliability pose legal and technical challenges.

India recently introduced three new criminal laws to replace colonial-era statutes:

1. Bharatiya Nyaya Sanhita (BNS), 2023
2. Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023
3. Bharatiya Sakshya Adhiniyam (BSA), 2023

These new laws aim to modernize the criminal justice system, particularly in handling cybercrimes and digital evidence. This paper examines legal challenges, new provisions, and their significance in Indian society.

2. Understanding Cybercrime and Digital Evidence

Cybercrime in the Digital Age

Cybercrimes involves illegal activities carried out using computers, networks, or the internet. Some common types include:

- **Hacking and Unauthorized Access** – Breaking into computer systems and databases.
- **Identity Theft and Data Breaches** – Misuse of personal data for illegal gains.
- **Cyber Terrorism** – Disrupting national security through digital means.
- **Online Harassment and Cyberbullying** – Defamation, threats, and stalking on social media.
- **Deepfake and AI Crimes** – Manipulating digital content for misinformation or fraud.

Digital Evidence in Legal Proceedings

Digital evidence includes:

- **Electronic records** – Emails, chat logs, social media posts.
- **Financial records** – UPI transactions, cryptocurrency logs.
- **Metadata and IP logs** – Device location, timestamps, forensic hash values.
- **Surveillance footage** – CCTV and smartphone videos.

Unlike physical evidence, digital evidence is **easily tampered with**, requiring strict legal safeguards.

3. New Legal Framework Governing Cybercrime and Digital Evidence

The **BNS, 2023**, introduces several new cybercrime-related provisions:

- **Section 163** – Identity theft, deepfake, and misuse of AI-based content.
- **Section 198(3)** – Cyberstalking, revenge porn, and cyberbullying.
- **Section 222** – Cyber terrorism, fake news propagation, and IT infrastructure attacks.

Significance:

- Recognizes **new-age cyber offenses** like AI-driven crimes, deepfake, and misinformation.
- Introduces **strict penalties** for cyber-related offenses, including imprisonment and fines.

Challenges:

- Needs effective enforcement by trained cybercrime police units.

BNSS, 2023 – Replacing CrPC, 1973

The **BNSS, 2023**, modernizes criminal procedure, particularly in cybercrime investigations. Key provisions include:

- **Section 176** – Digital evidence collection from social media and electronic records.
- **Increased Detention Periods** – Cybercrime suspects can be detained for **up to 90 days** (previously 60 days).

Significance:

- Streamlines the investigation of cybercrimes through electronic evidence.
- Allows for longer detention of cybercriminals, ensuring thorough digital forensics.

Challenges:

- Potential for misuse of detention provisions in cyber-related cases.
- Concerns over privacy violations and government overreach.

BSA, 2023

The **BSA, 2023**, modernizes the rules for admissibility of digital evidence:

- **Section 61** – Recognizes digital evidence, including blockchain-based records.

- **Section 63(2)** – Removes **strict certification requirements** under Section 65B (earlier mandatory).
- **Section 64** – Allows courts to accept electronic evidence without **a certificate from the producer**, if verified by forensic experts.

Significance:

- Makes **electronic evidence more admissible**, reducing **legal roadblocks** in cybercrime cases.
- Encourages **blockchain and AI-based evidence authentication**.

Challenges:

- Forensic infrastructure needs improvement to verify digital evidence effectively.
- Risks of forgery, manipulation, and deepfake usage in legal proceedings.

Challenges in Implementing Cybercrime Laws and Digital Evidence Framework

The introduction of Bharatiya Nyaya Sanhita (BNS), 2023, Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023, and Bharatiya Sakshya Adhiniyam (BSA), 2023 marks a major shift in India's legal approach to cybercrime and digital evidence. However, effective implementation faces several legal, technical, procedural, and infrastructural challenges. These challenges must be addressed to ensure the new laws achieve their intended objectives without infringing on civil liberties or causing delays in justice delivery.

1. Legal and Procedural Challenges

Complexity in Admissibility of Digital Evidence

- Although BSA, 2023 simplifies some aspects of digital evidence admissibility, courts may still struggle with verifying authenticity of electronic records.
- The removal of strict Section 65B certification requirements may create ambiguity in courts regarding the reliability of digital evidence.
- Judges and legal practitioners often lack technical expertise in handling digital evidence, leading to inconsistent rulings.

Jurisdictional Issues in Cybercrimes

- Cybercrimes often have cross-border implications, making jurisdiction a major issue.
- Indian law enforcement agencies face difficulties in obtaining data from foreign tech companies like Google, Meta, or Apple.
- Mutual Legal Assistance Treaties (MLATs) with other countries are often slow, leading to delays in cybercrime investigations.

Lack of a Dedicated Cybercrime Legal Framework

- While BNS, 2023 introduces provisions for cybercrimes, India lacks a comprehensive cybercrime law similar to the General Data Protection Regulation (GDPR) in the EU or the Computer Fraud and Abuse Act (CFAA) in the US.
- Existing cyber laws, such as the Information Technology Act, 2000, have not been updated to match modern AI-driven and blockchain-related cyber offenses.

2. Technical and Forensic Challenges

Difficulty in Tracing and Collecting Digital Evidence

- Digital evidence is volatile and can be easily altered, deleted, or encrypted by cybercriminals.
- Law enforcement agencies lack advanced forensic tools to retrieve encrypted or deleted data from cloud servers, dark web, and cryptocurrency transactions.
- The absence of blockchain-based authentication mechanisms makes it difficult to prove the integrity

of digital records.

Rising Threat of Deepfake and AI-Generated Misinformation

- Deepfake technology allows criminals to create manipulated images, videos, and voice recordings, which can be used for financial fraud, identity theft, and misinformation campaigns.
- The new laws do not explicitly address AI-generated evidence, raising concerns about proving authenticity and preventing misuse.

Cybersecurity Gaps in Government Infrastructure

- Many Indian government databases and law enforcement networks are vulnerable to cyberattacks, leading to leaks of sensitive citizen data.
- Cybercriminals exploit weak security measures to erase or manipulate evidence stored on public servers and police databases.

3. Investigative and Law Enforcement Challenges

Lack of Cyber Forensics Training for Police and Judiciary

- Most Indian police officers lack specialized training in handling cybercrime cases and digital forensics.
- Courts require expert forensic witnesses to verify digital evidence, but India faces a shortage of trained cybersecurity professionals.
- The bureaucratic delays in approving cybercrime investigations further slowdown justice delivery.

Overburdened Cybercrime Cells

- Indian cybercrime investigation units are understaffed and overburdened due to the rapid rise in online fraud, phishing, and hacking cases.
- There are only a few dedicated cyber police stations in major cities, making it difficult to address cases in rural and semi-urban areas.
- Cybercriminals exploit the slow response time of law enforcement agencies to avoid prosecution.

Need for Real-Time Data Access and Surveillance Regulations

- The BNSS, 2023 allows for extended detention of cybercrime suspects for up to 90 days, but there is no clear regulation on real-time digital surveillance.
- Law enforcement agencies struggle to obtain real-time access to encrypted communication platforms like WhatsApp, Telegram, and Signal, making cyber investigations more challenging.
- The lack of a clear Personal Data Protection Act (PDPA) raises concerns about potential privacy violations in cybercrime investigations.

4. Privacy and Ethical Concerns

Risk of Government Overreach and Mass Surveillance

- The BNSS, 2023 expands government powers to collect electronic records, but this raises concerns about surveillance abuse.
- There are fears that investigative agencies could misuse digital evidence collection powers to target activists, journalists, and political opponents.
- India currently lacks strong judicial oversight over government surveillance activities, increasing the risk of human rights violations.

Balancing National Security with Individual Privacy

- Cyber terrorism laws under BNS, 2023 allow stringent punishment for digital offenses related to national security, but vague definitions could lead to wrongful prosecutions.
- There is a need to define clear legal safeguards to prevent arbitrary arrests under cyber laws.

Encryption and Right to Privacy Conflicts

- While end-to-end encryption ensures user privacy, it prevents law enforcement agencies from accessing crucial evidence in cybercrime cases.
- Striking a balance between digital privacy and investigative requirements remains a major legal and ethical dilemma.

5. Case Studies and Judicial Precedents

Anvar P.V. v. P.K. Basheer (2014)

- Issue: Admissibility of electronic records without Section 65B certification.
- Judgment: Strict compliance with Section 65B required.
- Impact: Led to rejection of digital evidence in many cases.

Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020)

- Issue: Requirement of a certificate under Section 65B.
- Judgment: Reaffirmed strict compliance for digital evidence.
- Impact: Complicated cybercrime prosecutions due to lack of certification.

State (NCT of Delhi) v. Anurag Singh Bains (2021)

- Issue: Cyberstalking and online harassment.
- Judgment: Recognized WhatsApp chats and social media posts as valid evidence.

6. Recommendations for Effective Implementation

- **Develop Specialized Cybercrime Courts**: Establish fast-track courts for cybercrime cases with trained judges and forensic experts.
- **Enhance International Cooperation**: Strengthen extradition treaties and MLATs to enable cross-border investigations.
- **Introduce AI-Based Authentication of Digital Evidence**: Implement blockchain verification systems for preventing tampering of electronic records.
- **Train Law Enforcement and Judiciary**: Create mandatory cyber forensic training for police officers and judicial staff.
- **Ensure Judicial Oversight for Digital Surveillance:** Establish independent committees to monitor and prevent misuse of surveillance powers.
- **Expand Cybercrime Investigation Infrastructure**: Increase budget allocation for forensic labs, cyber police stations, and 24/7 cyber helplines.
- **Legislate a Comprehensive Cyber Law**: Enact a new cyber law framework to replace outdated provisions of the IT Act, 2000.
- **Cooperation for Cross-Border Cybercrimes:** Strengthen INTERPOL collaboration.
- **Legal Safeguards Against Misuse of Surveillance Powers:** Ensure privacy protection under the Personal Data Protection Act, 2023.

Conclusion

The new criminal laws of 2023 have significantly improved India's legal framework for cybercrime and digital evidence. While they offer greater admissibility of digital records, enhanced investigation powers, and stronger punishments, challenges remain in ensuring privacy, preventing evidence tampering, and updating laws to address emerging cyber threats. A balance between security and fundamental rights is crucial for an effective cyber legal regime in India the evolution of cybercrime and the increasing reliance

on digital evidence have necessitated a significant transformation in India's legal framework. With the enactment of Bharatiya Nyaya Sanhita (BNS), 2023, Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023, and Bharatiya Sakshya Adhiniyam (BSA), 2023, India has taken a proactive step toward modernizing its criminal justice system to address contemporary cyber threats and enhance the admissibility of digital evidence. These legal reforms replace outdated colonial-era laws and introduce provisions that recognize new-age cybercrimes, streamline investigation and prosecution mechanisms, and expand the scope of electronic evidence in court proceedings.

However, while these reforms mark significant progress, their effective implementation presents formidable challenges. Cybercriminals are constantly evolving, using sophisticated technologies such as artificial intelligence, deepfake manipulation, encrypted communications, and dark web networks to evade law enforcement. The sheer volume and complexity of digital evidence require advanced forensic tools, robust verification mechanisms, and well-trained personnel. Despite new legal provisions that facilitate the admissibility of electronic records, concerns about authenticity, reliability, and tampering remain. Courts and law enforcement agencies often lack technical expertise to assess and verify digital evidence effectively, which may lead to delayed trials and wrongful convictions.

Furthermore, jurisdictional issues in cross-border cybercrimes pose a significant hurdle. Many cybercriminals operate from foreign jurisdictions, making international cooperation and digital forensics collaboration crucial for effective prosecution. India's existing mutual legal assistance treaties (MLATs) are often slow and inefficient, hampering the investigation of transnational cybercrimes. Strengthening global alliances, data-sharing frameworks, and cybersecurity agreements is essential to address these challenges effectively.

In conclusion, while India's new legal framework lays a strong foundation for combating cybercrimes and improving the admissibility of digital evidence, its success depends on robust implementation, continuous policy refinement, and judicial adaptability. As cyber threats continue to evolve, the legal system must remain agile, technologically equipped, and globally aligned to effectively tackle emerging challenges. A well-balanced approach that prioritizes security, justice, and fundamental rights is essential for a resilient and future-ready cyber-legal ecosystem in India.