INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

DIGITAL EVIDENCE & CRIMINAL TRIALS: LEGAL CHALLENGES IN THE AGE OF ARTIFICIAL INTELLIGENCE

AUTHORED BY - MR. SAMBIK SARKAR
LL.B.(Honours) 2ND Year Student, University of Burdwan

ABSTRACT

We are living in a time when everything is going digital. This has led to a problem with cybercrime. The country is facing a challenge because of this. In todays world there are many bad things happening like hacking and financial scams and identity theft and cyber terrorism and crimes that use artificial intelligence. The country needs to have laws in place to deal with cybercrime. It also needs to have ways to investigate these crimes. Cybercrime is an issue and it includes things like hacking and financial scams and identity theft and cyber terrorism and crimes that use artificial intelligence. We need to have laws and good investigation mechanisms to deal with cybercrime. The Bharatiya Nyaya Sanhita or BNS that came out in 2023, the Bharatiya Nagarik Suraksha Sanhita which is also known as BNSS introduced in 2023 and the Bharatiya Sakshya Adhiniyam or BSA that was introduced in 2023 are bringing changes to the criminal justice system. These new laws are replacing the laws that were made during the colonial era and are also using the digital format. This is a time for the criminal justice system with the BNS, the BNSS and the BSA. The digital evidence and investigation process has been looked at from angles in the new Indian legal system. This is a topic because it affects people in many ways. There are bad things about digital evidence and investigation. For example, new laws have been made in India to help deal with crimes. These laws are helpful to law enforcement agencies because they are trying to stop cybercrime and other related crimes. Digital evidence and investigation are playing a role in this. In analysing the new Indian legal era, the focus is therefore on highlighting the relevance and utility of the new legal enactment coupled with its advantageous and detrimental attributes.

Keywords: India's 2023 criminal justice reforms under the Bharatiya Nyaya Sanhita (BNS), Bharatiya Nagarik Suraksha Sanhita (BNSS) and Bharatiya Sakshya Adhiniyam (BSA) now replace the colonial laws to effectively deal with increasing cybercrimes like hacking, financial

ISSN: 2582-6433

scams, identity theft, cyber terrorism and AI-related cybercrimes by highlighting evidence collected through digital investigation.

1. Introduction

Cybercrime has emerged to be one of the major concerns in India in the recent context of rapid digitization. Hacking, financial frauds, identity theft, cyber terrorism and other similar cybercrimes have thus necessitated developing appropriate legal standards in the process. Digital evidence plays one of the important roles in crime investigations. However, there are legal and technical challenges involving admissibility and authenticity in digital evidence.

India enacted three criminal law amendments recently to replace earlier statutes enacted during the colonial era:

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

The introduced laws seek to update the criminal justice system in regard to cybercrimes. This paper will attempt to discuss some of the legal challenges, new provisions that have been introduced and their relevance to Indian society.

1. A Simple Breakdown of Cybercrime and Digital Evidence

Cybercrime in the Digital Age

The Internet is a city with a lot of opportunities, thieves, bullies and tricksters. Internet crime can be described as any illicit hustle currently in play in the cyber world of computers, applications, etc. Here's the scoop:

- **Hacking:** Secretly entering someone else's cyber home, such as their bank site or email.
- **Identity Theft**: Where another person steals your identity pretends to be you, then proceeds to steal your money or ruin your reputation.
- **Cyber Terrorism**: This is where the big bad gets at a country's security; i.e., by hacking into their electrical grid.
- **Harassment/Cyber Bullying:** Spreading hate, threat or false statements on social media for harming someone emotionally.
- **Deepfakes/ AI Tricks**: Making use of AI for creating fake videos or speeches tricking people or disseminating wrong news.

ISSN: 2582-6433

Digital Evidence in Legal proceedings

Digital Evidence includes:

- Records that are Electronic(email messages, chats or instant messaging and social media).
- Records that are Financial(e-payment transactions through UPI and cryptocurrency).
- Recording of Digital Evidence Metadata and Logs of IP Addresses (where the digital device is located, when it was created as metadata, computed hashes for forensic use).
- Video or Image Recordings from Cameras that are Digital (CCTV and cell phone videos).
- Digital evidence is more susceptible to tampering than physical evidence of the crime requiring a much greater degree of legal protection from tampering.

3. New Legal Structure for Cyber Crime & Cyber Evidence

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

- **Section 163** - Crimes of identity theft, the use of deepfake technology and the misuse of artificial intelligence.
- **Section 198(3)** - Cyberstalking, revenge porn and cyberbullying offenses are prohibited.
- **Section 222** - Cyberterrorism, the spreading of false information and attacking IT infrastructure will be considered crimes under this section of The BNSS.

Significance:

- Identifying modern-day cyber-crimes. For example: Artificial Intelligence-based crime (such as forgeries); Deep fakes; Misinformation.
- Establishing stiff penalties for cyber crimes (imprisonment; fines).

Challenges:

- Must have structured enforcement by trained law enforcement agency (police) personnel who specialize in investigating & prosecuting cybercrimes.

BNSS, 2023 – Replaces Section 3 of CrPC, 1973

The BNSS, 2023 will update the criminal procedure to reflect modern technology used in investigating cyber crime and will include:

- Section 176 - Digital evidence will be collected from social media and from electronic records.

ISSN: 2582-6433

- Extended Detention Periods - A cyber crime suspect can be held for 90 days (previously 60 days).

Importance:

- Streamlining the investigation of cyber crimes using electronic evidence.
- Extending time an individual can be held when suspected of committing a cyber crime, allowing for more complete digital forensic work.

Challenges:

- Using or misusing the provisions for detention to her/his advantage in orders involving cyber related offences.
- Violating individuals' privacy and/or the potential for government overreaching with respect to previously mentioned digital content.

BSA, 2023

Modernisation of rules for admission of digital evidence under the BSA, 2023:

- Definition of digital evidence includes digital data and all forms of digital records (e.g. those that exist in a blockchain).
- Changes made to Section 63(2) remove strict certification of documents created under the authority of section 65B (the requirement is now not mandatory).
- Under section 64, courts may accept electronic evidence that has been verified by forensic experts as opposed to requiring certification from an electronic evidence creator.

Significance:

- Allows for the greater admission of electronic evidence into evidence and therefore reduces barriers in prosecuting cybercrime.
- Encouragement of blockchain technology to authenticate and validate evidence based on artificial intelligence.

Challenges:

- Forensic infrastructure needs improvement to allow for proper verification of digital evidence.
- Risks include forgery, manipulation and the use of deepfakes in legal proceedings.

Challenges in Implementing Cybercrime Laws and Digital Evidence Framework

The introduction of Bharatiya Nyaya Sanhita, Bharatiya Nagarik Suraksha Sanhita and

ISSN: 2582-6433

Bharatiya Sakshya Adhiniyam in 2023 is a change in how India deals with cybercrime and digital evidence.Putting these laws into action is not easy. There are problems that need to be solved so that the new laws can work as they should without hurting peoples rights or slowing down justice.

Legal And Procedural Challeneges

- Even though Bharatiya Sakshya Adhiniyam makes some things easier courts may still have trouble making sure electronic records are real.
- Not needing Section 65B certification anymore might make it unclear if digital evidence is reliable.
- Judges and lawyers often do not know enough about technology to handle evidence so they make different decisions.

Jurisdictial Issues In Cyber Crimes

- Cybercrimes can affect countries so it is hard to know which countrys laws to follow.
- Indian police have a time getting information from foreign companies like Google, Meta or Apple.
- It takes a time to get help from other countries, which slows down investigations into cybercrimes.

Deficiency in Cybercrime Legal Provisions

- Bharatiya Nagarik Suraksha Sanhita does talk about cybercrimes but India does not have a comprehensive law like the General Data Protection Regulation in the European Union or the Computer Fraud and Abuse Act in the United States.
- Current cyber laws, like the Information Technology Act are old. Do not cover new types of cybercrimes that use artificial intelligence and blockchain.

2. Techical and Forensic Challenges

Challenges Meet When Tracing And Gathering Digital Evidence

- Volatile Nature of Digital Evidence - Digital evidence is extremely delicate, meaning it can be altered/deleted or changed with ease by cybercriminals. This results in the challenge of preserving original information prior to it being compromised or destroyed.

ISSN: 2582-6433

- Limited Forensic Resources and Expertise - Many law enforcement agencies lack the technical resources and expertise needed to retrieve or restore encrypted data, especially from complex digital environments like the Cloud, the Dark Web and Cryptocurrency networks.
- Data Integrity Verification Challenges - Due to a lack of usable blockchain-based authentication techniques to verify digital records, it is often difficult to demonstrate that criminal digital records are authentic and have not been tampered with which creates problems when trying to present such evidence in a court of law.

Increasing Risk of Deepfake and AI-Generated Fake News

- Bad Use of Deepfake Technology - Cybercriminals use deep fake technology to create fake (but realistic) images, videos and audio recordings. These false materials may be used to commit legal crimes like financial fraud, identity theft, blackmail and false news.
- No Clear Legal Foundation for AI-Generated Evidence or Digital Images - Current law does not provide a clear set of rules to apply to AI-generated evidence or any other type of digital image or video footage. This creates uncertainty on how to verify authenticity of such digital evidence and raises worries about misuse in investigations or in court.

Gaps in Government Network Security

- **Government Databases' Susceptibility to Cyber Attacks** - Many government databases, particularly law enforcement databases in India, have vulnerabilities present where cyber criminals can take advantage of those gaps. These gaps will potentially lead to unauthorized access to sensitive personal data of citizens.
- **Tampering with/Deleting Digital Evidence -** Criminals could also take advantage of weak or insufficient network security to tamper with alter or delete digital evidence from public servers or police data bases; thereby preventing ongoing investigations and potentially jeopardizing the integrity of the justice system.

3. Investigative and Law Enforcement Difficulties

Limited Cyber Forensics Knowledge

- **Limited Training Opportunities -** Many Indian police officers are inadequately trained in dealing with various aspects of the investigation of cybercrime or cyber

ISSN: 2582-6433

forensics.

- **Lack of Training Opportunities** - The courts require that a qualified forensic witness provide expert testimony related to cybercrimes; however, there is currently a shortage of trained cybersecurity professionals to fill that role.
- **Bureaucratic Roadblocks** - Bureaucratic constraints often impede the timely resolution of cases related to cybercrime, due to the prohibitive length of time required for obtaining approval from the government to conduct cybercrime investigations.

Congested Cybercrime Units

- **Rapid Increase** - The cybercrime units are often overwhelmed because of an immense increase in online fraud, phishing and hacking-related cases; as a result, there are many more cases than available personnel to investigate them.
- **Limited Number of Cyber Police** - Dedicated cyber police stations are located only in large cities, making it difficult to respond to or investigate in rural and semi-urban areas.
- **Delayed Response from Law Enforcement -** The slow response of police departments often allows cybercriminals to avoid detection.

Real-time Data Retrieval and Surveillance Regulation Issues

- **Vague Definition of Surveillance** – The Bharatiya Nagarik Suraksha Sanhita of 2023 provides longer periods of detention for individuals accused of cybercrime. However, there are no clearly defined rules governing real-time digital surveillance of individuals suspected of cybercrime.
- **Encrypted Platforms** - Investigators are unable to access encrypted platforms such as WhatsApp, Telegram and Signal which further complicates the investigative process.
- **Potential Violations of Privacy** - Failure to adopt a comprehensive Personal Data Protection Act (PDPA) raises concerns about privacy violations in the course of investigating cybercrime.

4. Concerns Regarding Privacy and Ethics

Mass Surveillance and Government Overreach Risks

- **Increased Surveillance Authority** - The Bharatiya Nagarik Suraksha Sanhita, 2023 allows for greater access of electronic records to officials; this raises fears of the

ISSN: 2582-6433

overreach of authority in abusing these powers to conduct excessive amounts of surveillance.

- **Possible Misuse of Authority -** There is concern that agencies charged with investigating would misuse their authority to conduct investigations on individuals who they believe to be activists, journalists or political opposition.
- **Judicial Oversight is Limited -** There are not sufficient amounts of judicial oversight protecting the rights of individuals from human rights abuses related to the potential abuse of surveillance laws.

Individual Privacy vs National Security

- **Stringent Cybercrime Provisions** - The Bharatiya Nyaya Sanhita, 2023 sets forth severe penalties for violations against cybercrimes that threaten national security; however, the definitions of what constitutes cybercrime may be vague and could lead to individuals being prosecuted erroneously.
- **Legal Protection Needed** - There will be a need for appropriate legal protections which to protect against arbitrary arrests and individual privacy rights.

Encryption vs Right to Privacy

- **Difficulty Accessing Evidence -** End-to-end encryption provides individuals with protection of their digital privacy; however, it can serve as a barrier preventing law enforcement from accessing critical digital pieces of evidence when investigating cybercrime.
- **Ethical Dilemma** - The need to balance the need for protection of an individual's digital privacy vs law enforcement's ability to conduct investigations into crimes is both an ethical and legal issue.

5. Case Studies of Judicial Precedent

1. State (NCT of Delhi) Vs. Navjot Sandhu (2005)

Issue:

The admissibility of electronic records such as phone call data and computer records in criminal trial.

Judgment:

The Supreme Court allowed electronic records such as call logs and data from computers to be

ISSN: 2582-6433

admitted into evidence without having produced a Section 65B certificate.

Importance/Impact:

• The case established flexibility for the admission of electronic records; however, the rationale of this case was later criticized and effectively overruled in later decisions (Anvar P.V. Vs P.K. Basheer); therefore, strict compliance with Section 65B was required.

Research Significance:

The case indicates early judicial efforts by the courts to admit electronic records into evidence before strict rules existed regarding the same.

2. Tomaso Bruno v. State of Uttar Pradesh (2015)

Issue:

Whether failure to produce electronic evidence such as CCTV footage **could affect the prosecution's case.**

Judgment:

The Supreme Court held that electronic evidence plays an important role in modern investigations **and courts should not ignore technological tools like CCTV recordings.**

Impact:

- **The Court emphasized that** modern crimes must be investigated using modern technology**.**
- **It encouraged the use of digital records such as CCTV, emails and electronic documents in criminal trials.**

Research Significance:

This case highlighted the growing importance of digital evidence in criminal justice**.**

3. Shafhi Mohammad v. State of Himachal Pradesh (2018)

Issue:

Whether the Section 65B certificate is always mandatory **for electronic evidence.**

Judgment:

The Supreme Court ruled that the certificate requirement can be relaxed in certain circumstances**, especially when the person presenting the evidence does not have control over the device from which the record was produced.**

Impact:

- **The Court attempted to make the law** more practical for investigators and litigants**.**
- **However, this view was later** overruled by the Supreme Court in ***Arjun Panditrao***

ISSN: 2582-6433

***Khotkar v. Kailash Kushanrao Gorantyal (2020)*, which reinstated strict compliance with Section 65B.**

Research Significance:

This case reflects the judicial debate on flexibility vs. strict procedural compliance in digital evidence law.

4. Sanjaysinh Ramrao Chavan v. Dattatray Gulabrao Phalke (2015)

Issue:

Authenticity and admissibility of electronic records in election-related litigation.

Judgment:

The Supreme Court emphasized that source and authenticity are the two most important factors when evaluating electronic evidence**.**

Impact:

- **Reinforced the principle that** electronic evidence must be properly authenticated **before being admitted in court.**

Research Significance:

The case strengthened the judicial focus on reliability and authenticity of digital evidence.

6. Recommendations for Effective Implementation

- **Establishment of Specialized Cybercrime Courts**

  In view of the growing complexity of cyber-related offences, it is recommended that specialized cybercrime courts be established. These courts should function as fast-track forums dedicated exclusively to cybercrime cases. Judges presiding over such courts should receive specialized training in digital forensics, cyber law and electronic evidence to ensure efficient adjudication and timely delivery of justice.

- **Strengthening International Co-operation Mechanism**

  Cybercrime frequently transcends national borders, making international collaboration essential for effective enforcement. Governments should enhance cooperation through stronger extradition treaties, Mutual Legal Assistance Treaties (MLATs) and joint investigative mechanisms. Improved coordination with international law enforcement agencies will facilitate evidence sharing, suspect identification and prosecution of offenders operating across jurisdictions.

ISSN: 2582-6433

- **Adoption of Advanced Technology for Digital Evidence Authentication**

  To ensure the integrity and reliability of electronic records, advanced technological solutions should be implemented. The use of artificial intelligence-based authentication systems and blockchain technology can help create tamper-proof records, thereby strengthening the evidentiary value of digital data presented before courts.

- **Capacity Building for Law Enforcement and the Judiciary**

  Effective enforcement of cyber laws requires well-trained personnel. Mandatory training programs in cyber forensics, digital investigation techniques and electronic evidence management should be introduced for police officers, prosecutors and judicial officers. Regular workshops and certification programs can significantly improve institutional capacity to address technologically sophisticated crimes.

- **Ensuring Judicial Oversight over Digital Surveillance**

  While digital surveillance tools are often necessary for investigating cyber offences, their use must be balanced with the protection of civil liberties. Establishing independent oversight mechanisms or review committees can help ensure that surveillance powers are exercised lawfully and proportionately, preventing misuse or arbitrary intrusion into individuals' privacy.

- **Expansion of Cybercrime Investigation Infrastructure**

  Governments should allocate greater financial and technical resources toward strengthening cybercrime investigation infrastructure. This includes establishing more cyber forensic laboratories, expanding dedicated cyber police stations and maintaining round-the-clock cybercrime helplines to assist victims and facilitate prompt reporting of offences.

- **Development of a Comprehensive and Updated Cyber Law Framework**

  Given the rapid pace of technological advancements, certain provisions of the existing legal framework require modernization. Legislators should consider developing a comprehensive cyber law regime that addresses emerging threats such as artificial intelligence-driven crimes, data breaches, digital identity theft and cryptocurrency-related offences.

ISSN: 2582-6433

- **Enhanced Global Co-operation in Combating Cybercrime**

  Effective response to cybercrime requires coordinated global efforts. Strengthening collaboration with international policing organizations such as INTERPOL can facilitate intelligence sharing, coordinated investigations and the tracking of cybercriminal networks operating in multiple jurisdictions.

- **Legal Safeguards Against Misuse of Surveillance Powers**

  Robust legal safeguards must be established to ensure that investigative powers do not undermine individual privacy rights. Data protection legislation, such as the Digital Personal Data Protection Act, 2023, should be implemented effectively to regulate the collection, storage and processing of personal data while maintaining accountability and transparency in digital surveillance practices.

Conclusion

The new criminal laws introduced in 2023 have significantly modernized India's legal framework for dealing with cybercrime and digital evidence. With the implementation of the Bharatiya Nyaya Sanhita, 2023, Bharatiya Nagarik Suraksha Sanhita, 2023 and Bharatiya Sakshya Adhiniyam, 2023, India has taken an important step toward replacing outdated colonial-era laws with provisions that better reflect the realities of a digital society. These reforms recognize modern cybercrimes, improve investigation and prosecution processes and broaden the scope for admitting electronic evidence in court. However, implementing these laws effectively remains a challenge. Cybercriminals are constantly adopting advanced technologies such as artificial intelligence, deepfakes, encrypted platforms and dark-web networks, which makes detection and investigation more complex. The growing volume of digital evidence also requires advanced forensic tools, proper verification systems and well-trained investigators. Without adequate technical expertise among law-enforcement agencies and courts, questions about the authenticity and reliability of electronic evidence may lead to delays or errors in the justice process. Another major challenge is jurisdiction in cross-border cybercrimes. Many cyber offences originate outside India, making international cooperation essential. Existing mechanisms like Mutual Legal Assistance Treaties (MLATs) often take time, which can slow down investigations. Strengthening global partnerships, improving data-sharing frameworks and enhancing cybersecurity cooperation will therefore be crucial.

ISSN: 2582-6433

Overall, the new legal framework provides a strong foundation for addressing cybercrime and improving the use of digital evidence in India's justice system. However, its true effectiveness will depend on proper implementation, regular legal updates, technological capacity and skilled personnel. Maintaining a balance between security, justice and fundamental rights will be essential to build a strong and future-ready cyber-legal system in India.