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

Critical analysis on Overlap between the Information Technology Act, 2000 and the Bharatiya Nyaya Sanhita, 2023 in Regulating Cyber Offences: A Critical Legal Analysis

Shobhit Seth[1], Dr. Jyoti Yadav[2]

[1]Student, LLM in Cyber Laws and Cyber Securities, Amity Law School, Amity University Lucknow Campus
[2]Assistant Professor, Amity Law School, Amity University Lucknow Campus

Abstract
The nature and extent of criminal activity have changed dramatically as a result of society's rapid digitalization. Due to the extensive use of the internet, digital payments, and social media platforms, cybercrimes like identity theft, online fraud, hacking, cyber harassment, and financial frauds have become more common in India. The Information Technology Act, 2000, which establishes penalties for various cyber-related crimes and gives legal recognition to electronic transactions, is the main piece of legislation governing cyber offenses in India. The Indian Penal Code was recently replaced by the Bharatiya Nyaya Sanhita, 2023, which contains several provisions pertaining to identity theft, fraud, and communication-based offenses that may also be applicable in cyberspace. Because of this overlap, cybercrimes may be covered by both statutes at the same time, creating a complicated legal framework. The current study evaluates the need for harmonization within India's cybercrime regulatory framework, critically analyses the overlapping provisions of the Information Technology Act and the Bharatiya Nyaya Sanhita, and considers their practical implications for law enforcement and judicial interpretation. The study comes to the conclusion that although having these laws together strengthens the legal framework against cybercrime, more precise legislative coordination is required to prevent confusion and guarantee efficient enforcement.

Keywords: Cyber law. Digital Evidence, Criminal Law Reform. Digital Criminal Law Cyber Jurisdiction

1. Introduction

The global socio-economic landscape has been profoundly reshaped by the rapid growth of digital technology. Today, digital communication, online transactions, and internet connectivity have become indispensable aspects of everyday life. In India, this transformation has been particularly significant, driven by initiatives such as the Digital India programme, expansion of internet infrastructure, and the widespread adoption of digital payment systems. While these advancements have brought convenience and efficiency, they have also given rise to increasingly complex forms of cybercrime. Cybercrime broadly

[1] Student, LLM in Cyber Laws and Cyber Securities, Amity Law School, Amity University Lucknow Campus
[2] Assistant Professor, Amity Law School, Amity University Lucknow Campus

refers to unlawful activities carried out using computers, digital devices, or networks. These include offenses such as hacking, phishing, identity theft, cyberstalking, online financial fraud, ransomware attacks, and data breaches. The borderless nature of the internet and the anonymity it offers to offenders make cybercrime especially challenging for law enforcement agencies to detect and control. In response to these emerging threats, India enacted the Information Technology Act, 2000, which serves as the primary legal framework governing electronic transactions and cyber-related offenses.[3] The Act addresses key issues such as computer-related crimes, data protection, and the legal recognition of digital signatures. More recently, India undertook a comprehensive reform of its criminal laws through the introduction of the Bharatiya Nyaya Sanhita, 2023, which replaced the Indian Penal Code.[4] Although the Bharatiya Nyaya Sanhita is not specifically designed to regulate cybercrime, several of its provisions relating to cheating, fraud, defamation, and criminal intimidation can be applied to offenses committed through digital means. The coexistence of these two legal frameworks has led to areas of overlap in the regulation of cyber offenses. Certain acts committed in the digital space may fall within the scope of both the Information Technology Act and the Bharatiya Nyaya Sanhita. This overlap raises important legal questions regarding jurisdiction, statutory interpretation, and the application of criminal liability. Accordingly, this paper seeks to critically examine the extent of such overlap and assess whether it strengthens or complicates the regulation of cybercrime in India.

2. The Architecture of India's Cyber Law

The evolution of cyber law in India reflects the country's gradual adaptation to the challenges posed by the digital age. In the initial stages of technological growth, it became evident that traditional legal frameworks were not equipped to deal with crimes committed in virtual environments. As electronic commerce began expanding rapidly in the late 1990s, the need for a legal system that could recognise electronic records and validate digital transactions became increasingly urgent. Address this gap, India enacted the Information Technology Act, 2000, which marked a significant milestone in the country's legal history. The legislation was inspired by the UNCITRAL Model Law on Electronic Commerce and aimed to provide legal recognition to electronic records and digital signatures.[5] It also introduced provisions to penalise unauthorised access to computer systems, data theft, and other emerging forms of cyber offences. As technology continued to evolve, so did the nature of cybercrime. Recognising the limitations of the original Act, the government introduced the Information Technology (Amendment) Act, 2008. This amendment significantly broadened the scope of cyber law by incorporating offences such as identity theft, cheating by personation using computer resources, and violations of privacy.[6] These changes enhanced India's capacity to effectively investigate and prosecute cyber offenders, while also bringing its legal framework closer in line with global standards.

[3] *Information Technology Act, No. 21 of 2000, Acts of Parliament, 2000 (India).*
[4] *Bharatiya Nyaya Sanhita, No. 45 of 2023, Acts of Parliament, 2023 (India).*
[5] *Information Technology Act, No. 21 of 2000, Acts of Parliament, 2000 (India); UNCITRAL Model Law on Electronic Commerce, G.A. Res. 51/162, U.N. Doc. A/RES/51/162 (Jan. 30, 1997).*
[6] *Information Technology (Amendment) Act, No. 10 of 2009, Acts of Parliament, 2009 (India).*

Despite the presence of a specialised cyber law regime, traditional criminal law provisions have continued to play a complementary role. Offences involving fraud, deception, defamation, and criminal intimidation—when committed through digital platforms—can still be prosecuted under general criminal law. With the enactment of the Bharatiya Nyaya Sanhita, 2023, this dual framework has become even more pronounced, highlighting the overlapping application of cyber-specific and general criminal laws in India.

3. The Nature of the Overlap: Special vs. General Law

The overlap between the Information Technology Act, 2000 and the Bharatiya Nyaya Sanhita, 2023 can best be understood through the legal distinction between lex specialis (special law) and lex generalis (general law). While both statutes operate in the field of criminal law, they differ significantly in their scope, focus, and application. This dual framework often leads to practical as well as interpretational challenges.

4. The IT Act as Lex Specialis

The Information Technology Act, 2000 functions as a special law, specifically designed to address offences that arise within digital environments. Its provisions are technologically oriented and apply where a computer system, network, or digital device is either the target or the primary tool of the offence. For instance, Sections 43 and 66 deal with unauthorised access, data theft, and hacking-related activities, requiring proof that the offence involved a computer resource.[7] Section 66C specifically criminalises identity theft involving digital credentials such as passwords or electronic signatures.[8] Similarly, Section 66D addresses cheating by personation carried out through computer resources, a provision frequently used in phishing and online fraud cases. What distinguishes these provisions is their technical specificity—the prosecution must establish not only the wrongful act but also the use of a digital medium as an essential element of the offence.

[7] *Information Technology Act, No. 21 of 2000, sec 43, 66, Acts of Parliament, 2000 (India).*
[8] *Information Technology (Amendment) Act, No. 10 of 2009, § 66C, Acts of Parliament, 2009 (India).*

4. Ground-Level Issues from the Initial Stage

1. Filing of FIR

- Confusion at police station regarding applicable law
- Uncertainty whether to apply Information Technology Act, 2000, Bharatiya Nyaya Sanhita, 2023, or both.
- Practice of "overcharging" (adding multiple sections to be safe)
- FIRs become cluttered with numerous provisions.
- Leads to lack of clarity and confusion from the very beginning.

2. Investigation Stage

- IT Act requires proof of technical elements (e.g., unauthorised access, computer resource misuse)
- Requires digital forensic expertise.
- Lack of trained personnel in most police stations
- Investigators rely on traditional methods (confession-based approach)
- Failure to collect crucial digital evidence (IP logs, metadata, server data)
- Weakens prosecution case → may result in acquittal.

3. Judicial Observation

- Courts have acknowledged investigation gaps.
- Karnataka High Court termed it a "lamentable reality".
- Observed that conventional officers are ill-equipped to manage cybercrimes.

5. The BNS as Lex Generalis

In contrast, the Bharatiya Nyaya Sanhita, 2023 operates as the general criminal law of the country. It focuses on the nature of the offence—such as cheating, intimidation, or defamation—without being concerned about the medium through which the act is committed. For example, Section 318 of the BNS defines the offence of cheating, which may include online frauds when committed through digital platforms[9]. Section 351 deals with criminal intimidation, which can extend to threats issued via emails, social media, or messaging applications[10]. Similarly, provisions relating to defamation (e.g., Sections 79–80 BNS) apply equally to defamatory statements published online. Thus, the BNS criminalises the result or effect of an act, regardless of whether it occurs in physical or digital space.

Ground-Level Issues from Investigation to Court

One of the major challenges in cybercrime cases arises during the investigation stage, where confusion among investigators often leads to ineffective enforcement. Since offences under the Bharatiya Nyaya Sanhita, 2023—such as cheating and criminal intimidation—are more familiar to law enforcement, there is a tendency to rely heavily on these provisions while neglecting the technical requirements of the Information Technology Act, 2000. In many instances, charge sheets are drafted primarily under provisions like Section 318 (cheating) and Section 351 (criminal intimidation) of the BNS, without adequately establishing the digital elements required under provisions such as Section 66D of the IT Act. This results in superficial or incomplete investigations. Legal experts have repeatedly pointed out that the quality of investigation in cyber offences remains a "major fault-line," often leading to miscarriage of justice.[11]Another significant issue relates to jurisdiction. Cybercrimes transcend geographical boundaries,

[9] *Bharatiya Nyaya Sanhita, No. 45 of 2023, sec 318, Acts of Parliament, 2023 (India).*
[10] *Id. sec 351.*
[11] *See, expert commentary on deficiencies in cybercrime investigation in India.*

and the IT Act and the BNS address this aspect differently, leading to practical complications. Section 1(5) of the BNS extends its applicability to offences committed outside India if they target a computer resource located within India. In comparison, Section 75 of the IT Act has a broader scope, applying to offences committed outside India as long as they involve a computer, system, or network located in India.

This creates complex jurisdictional dilemmas in real-world scenarios. For instance, if a cyber fraudster based in Dubai sends a phishing email to a victim in Mumbai through servers located in Europe, determining the place of occurrence of the offence becomes difficult. Although Indian authorities may register the case, securing the presence of the accused located abroad becomes challenging due to the principle of dual criminality, which requires that the act must also be recognised as an offence in the foreign jurisdiction. Courts have grappled with such issues; for example, the Gujarat High Court cyber jurisdiction cases have dealt with cases where accused persons located in foreign jurisdictions contested the territorial jurisdiction of Indian authorities[12].

The overlap between the two statutes also raises concerns regarding double jeopardy. Since the same act—such as hacking a bank server—may fall under both the IT Act (for unauthorised access) and the BNS (for cheating or fraud), there is a risk of prosecuting an individual twice for the same offence. The Bombay High Court double jeopardy observations has strongly criticised this practice, describing it as a violation of the constitutional protection under Article 20(2) against double jeopardy.[13] The Court emphasised that when a special law like the IT Act applies, invoking general criminal law provisions for the same set of facts is inappropriate. However, in practice, law enforcement agencies often invoke both statutes simultaneously, leading to prolonged legal disputes over the validity of charges. A related concern arises in the context of bail. Offences under the IT Act, such as those under Section 66, are bailable and compoundable, with comparatively lighter punishments. In contrast, offences like cheating under Section 318 of the BNS are non-bailable and carry more severe penalties, including imprisonment of up to seven years.

This difference creates a strategic issue at the ground level. It is often argued that investigators deliberately include harsher BNS provisions alongside IT Act offences to make it more difficult for the accused to obtain bail. As a result, an offence that would ordinarily be bailable under the IT Act may effectively become non-bailable, leading to prolonged pre-trial detention. The Jharkhand High Court bail in cyber offences has recently considered such situations, where extended custody of the accused became a relevant factor in granting bail.[14]This highlight how procedural overlap can have serious implications for personal liberty.

6. Overlapping Legal Frameworks in Cybercrime Regulation and Judicial Response

The regulation of cybercrime in India reflects a complex interaction between the Information Technology Act, 2000 and the Bharatiya Nyaya Sanhita, 2023. While the former is a specialised statute dealing specifically with digital offences, the latter provides a broader framework of criminal liability. This dual structure has led to significant areas of overlap, interpretational challenges, and evolving judicial responses.

6.1 Areas of Overlap between the IT Act and BNS

Several categories of cyber offences demonstrate how both statutes may simultaneously apply.

[12] *See, decisions of the Gujarat High Court dealing with extraterritorial jurisdiction in cybercrime cases (India).*
[13] *See, observations of the Bombay High Court on double jeopardy in overlapping offences (India).*
[14] *See, recent bail orders of the Jharkhand High Court in cybercrime matters (India).*

Online Fraud and Financial Scams

Digital fraud, including phishing emails, fake websites, and fraudulent online transactions, represents one of the most common cyber offences. Such acts fall within computer-related offences under the IT Act while also constituting "cheating" under the BNS. The dual applicability often leads to parallel invocation of provisions, depending on the nature and evidence of deception involved.[15]

Identity Theft

Identity theft, particularly involving the misuse of passwords, digital signatures, or biometric data, is specifically addressed under Section 66C of the IT Act. However, the same conduct may also amount to impersonation or fraud under general criminal law provisions in the BNS.[16]

Cyber Harassment and Stalking

Offences such as cyberstalking, online threats, and harassment through social media platforms fall at the intersection of both statutes. While the IT Act addresses unauthorised access and misuse of communication systems, the BNS criminalises acts causing fear, intimidation, or harm to an individual's dignity.

Digital Defamation

Defamatory content published online raises another instance of overlap. While the IT Act governs intermediary liability and electronic publication, the substantive offence of defamation continues to be prosecuted under criminal law provisions of the BNS.[17]

6.2 Judicial Interpretation and Constitutional Safeguards

The Indian judiciary has played a transformative role in harmonising cyber law with constitutional guarantees. Courts have consistently emphasised that technological regulation must not come at the cost of fundamental rights. [18]A landmark judgment in this regard is Shreya Singhal v. Union of India, where the Supreme Court struck down Section 66A of the IT Act. The Court held that the provision was vague, overbroad, and had a chilling effect on free speech, thereby violating Article 19(1)(a) of the Constitution. The judgment clarified the distinction between permissible restrictions and unconstitutional limitations, particularly in the context of online expression. It also reinforced the principle that criminal law must be precise and narrowly tailored when dealing with speech-related offences. Subsequent judicial decisions have continued to shape cyber jurisprudence by interpreting intermediary liability, evidentiary standards in digital crimes, and the scope of investigative powers in cyberspace.

6.3 Role of the Safe Harbour Principle

An essential feature of the IT Act is the incorporation of the "safe harbour" principle under Section 79. This provision grants conditional immunity to intermediaries—such as social media platforms, internet service providers, and hosting services—for third-party content hosted on their platforms. The scope of this protection was significantly clarified in Shreya Singhal v. Union of India,[19] where the Supreme Court held that intermediaries are required to remove unlawful content only upon receiving a court order or government notification. This interpretation ensures a balance between regulating harmful online content and preventing excessive censorship by private entities. The safe harbour principle thus acts as a safeguard for digital innovation and freedom of expression while imposing a duty of due diligence on intermediaries. However, the interaction between safe harbour protections and criminal liability under the BNS remains

[15] *Information Technology Act, 2000, sec 43, 66; Bharatiya Nyaya Sanhita, 2023 (cheating provisions).*
[16] *Information Technology Act, 2000, sec66C.*
[17] *Bharatiya Nyaya Sanhita, 2023 (defamation provisions).*
[18] *Information Technology Act, 2000, sec 79; Shreya Singhal v. Union of India, (2015) 5 SCC 1.*
[19] *Shreya Singhal v. Union of India, (2015) 5 SCC 1.*

a grey area, particularly when intermediaries are alleged to have facilitated or failed to prevent criminal conduct.

6.4 Challenges Arising from Overlapping Legal Frameworks

The coexistence of the Information Technology Act, 2000 and the Bharatiya Nyaya Sanhita, 2023 has led to a range of practical and legal challenges in the regulation of cyber offences. One of the primary concerns is the uncertainty faced by law enforcement agencies in deciding whether to apply specialised provisions under the IT Act or rely on the broader criminal framework of the BNS. This ambiguity often results in inconsistent application of the law and, in some cases, duplicative charges for the same conduct. Additionally, the overlap between these statutes raises important concerns regarding the principle of double jeopardy, as there is a possibility that a single act may be prosecuted under multiple legal provisions. In such situations, courts are required to carefully examine whether the offences in question are distinct in their ingredients or merely repetitive in nature. Another significant issue is the lack of technical expertise within traditional policing systems. Cybercrime investigations demand specialised skills in areas such as digital forensics, encryption technologies, and data analysis. However, the absence of adequate training and infrastructure often weakens the quality of investigation and ultimately affects the success of prosecution. Furthermore, the rapid pace of technological advancement continues to outstrip the existing legal framework. New and sophisticated forms of cybercrime, including cryptocurrency fraud, deepfake technology, and artificial intelligence-driven scams, pose serious challenges to both the IT Act and the BNS, as these laws struggle to adapt to the constantly evolving digital landscape.

SUGGESTIONS AND RECOMMENDATIONS

Enact a Clear Legislative Demarcation Clause

- Parliament should introduce an explicit “non-obstante + harmonisation clause” clarifying when the IT Act will prevail over BNS provisions in cyber offences.
- This avoids duplication and forum-shopping by investigators.
- Illustration:
  If a phishing scam involves unauthorized system access + cheating, the law should clearly state:
- IT Act governs the technical offence (data breach)
- BNS applies only for ancillary consequences (cheating, fraud)
- Comparative Insight:
- European Union uses the principle of lex specialis under instruments like the NIS Directive, where specialised cyber laws override general criminal law.
  Develop Unified Cybercrime Charging Guidelines
- The Ministry of Home Affairs should issue standardised prosecution guidelines for police and prosecutors.
- These should specify:
  - When to invoke IT Act vs BNS
  - When both can be applied without violating double jeopardy
- Illustration:
  A social media fraud case:
- IT Act for unauthorized access
- BNS only if independent elements like inducement or wrongful loss are proven

- Comparative Insight:
- In the United States, the Computer Fraud and Abuse Act is applied alongside general fraud statutes, but Department of Justice guidelines prevent overcharging.
  Strengthen Protection Against Double Jeopardy
- Courts should evolve a "same transaction + distinct ingredients test" for cyber offences.
- Legislative clarification may be added to reflect Article 20(2) protections.
- Illustration:
  If identity theft (IT Act sec66C) and cheating (BNS) arise from the same act:
- Only one punishment unless elements are legally distinct
- Comparative Insight:
- The United Kingdom applies strict tests under the Computer Misuse Act 1990 and general criminal law to avoid duplicative punishment.
  Establish Specialised Cybercrime Units and Courts
- Create dedicated cybercrime investigation units with:
  - Digital forensic labs
  - Blockchain analysis tools
  - AI-based threat detection
- Establish special cyber courts for faster adjudication.
- Illustration:
  A cryptocurrency scam investigation requires blockchain tracing tools—traditional police stations are unequipped for this.
- Comparative Insight:
- Estonia has advanced cybercrime units and digital governance infrastructure, enabling faster and more efficient prosecutions.
  Capacity Building and Mandatory Training
- Introduce compulsory certification programs in cyber forensics for:
  - Police officers
  - Prosecutors
  - Judicial officers
- Illustration:
  Incorrect handling of digital evidence (e.g., improper chain of custody) often leads to acquittals.
- Comparative Insight:
- The Europol conducts specialised cyber training programs for member states.
  Update the IT Act to Address Emerging Technologies
- Amend the IT Act to explicitly regulate:
  - AI-generated crimes (deepfakes)
  - Cryptocurrency fraud
  - Dark web transactions
- Illustration:
  Deepfake videos used for extortion currently fall into grey areas between defamation and fraud laws.
- Comparative Insight:
- The European Union is proactively regulating AI through frameworks like the AI Act.

Clarify and Strengthen Safe Harbour Provisions

- Clearly define intermediary liability under Section 79:
  - Introduce graded liability (passive vs active intermediaries)
  - Mandate time-bound compliance mechanisms.
- Illustration:
  A social media platform should not be liable for user content unless it fails to act after legal notice.
- Comparative Insight:
- In the United States, Section 230 of the Communications Decency Act provides broad immunity but is now evolving with accountability debates.
  "Cyber Offence Classification Framework"
- Categorise offences into:
  - Core cyber offences → governed by IT Act
  - Cyber-enabled traditional offences → governed by BNS
- Illustration:
- Hacking → IT Act
- Online cheating → BNS
- Hybrid offences → dual but regulated application
- Promote Inter-Agency Coordination Mechanisms
- Establish a centralised cybercrime coordination authority integrating:
  - Police
  - CERT-In
  - Financial intelligence units
- Illustration:
  A ransomware attack involves banking fraud, data breach, and extortion—multiple agencies must coordinate.
- Comparative Insight:
- The United States uses joint task forces like FBI cyber divisions for coordinated responses.
- Encourage Judicial Guidelines and Precedent Development
- The Supreme Court should issue authoritative guidelines on:
  - Overlapping offences
  - Evidentiary standards in cybercrime
  - Intermediary liability
- Illustration:
  The ruling in Shreya Singhal v. Union of India clarified free speech and safe harbour—similar clarity is needed for overlap issues.
  (Key Takeaway)
- A balanced approach is required—not complete separation, but structured harmonisation. India must move towards:
- Clear legislative hierarchy
- Technically equipped enforcement
- Rights-oriented judicial interpretation

- Only then can the overlap between the IT Act and BNS become a strength rather than a source of legal uncertainty.

Conclusion

The coexistence of the Information Technology Act, 2000 and the Bharatiya Nyaya Sanhita, 2023 reflects India's attempt to address cybercrime through both specialised and general criminal law frameworks. While this dual structure offers flexibility in prosecuting offences, it simultaneously gives rise to significant legal and practical challenges. The overlapping provisions often create uncertainty for law enforcement agencies, leading to inconsistent charging practices and, at times, duplication of offences. This not only complicates investigations but also raises constitutional concerns, particularly in relation to the principle of double jeopardy.

Furthermore, the rapid evolution of technology continues to test the limits of existing legal frameworks. Emerging forms of cybercrime such as artificial intelligence-based frauds, deepfakes, and cryptocurrency-related offences expose gaps in both statutes, highlighting the urgent need for legislative adaptation. At the same time, the lack of technical expertise and infrastructure within investigative agencies undermines the effective enforcement of cyber laws, often resulting in weak prosecution and low conviction rates.

Judicial intervention has played a crucial role in mitigating some of these challenges. Decisions such as Shreya Singhal v. Union of India have reinforced the importance of safeguarding fundamental rights while regulating cyberspace. However, reliance on judicial interpretation alone is insufficient to resolve systemic issues arising from legislative overlap.

In this context, a balanced and harmonised approach is essential. Clear statutory guidelines, improved inter-agency coordination, capacity building, and timely legal reforms are necessary to ensure that the overlap between the IT Act and the BNS does not hinder justice delivery. Instead, it should function as a complementary framework capable of effectively addressing the complexities of cybercrime while upholding constitutional values and the rule of law in the digital age.

Bibliography

Primary Sources

Legislation

1. Information Technology Act, 2000.
2. Bharatiya Nyaya Sanhita, 2023.
3. Constitution of India, 1950.
4. Computer Misuse Act 1990.
5. Computer Fraud and Abuse Act.
6. NIS Directive.
7. AI Act.

Cases

1. Shreya Singhal v. Union of India, (2015) 5 SCC 1.
2. Avnish Bajaj v. State (NCT of Delhi), 150 (2008) DLT 769.
3. State of Tamil Nadu v. Suhas Katti.
4. K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.

Secondary Sources

Books

1. Nir Kshetri, Cybercrime and Cybersecurity in India (Springer, 2013).
2. Debarati Halder & K. Jaishankar, Cyber Crime and the Victimization of Women (SAGE, 2011).
3. Kamath Nandan, Law Relating to Computers, Internet and E-Commerce (Universal Law **Publishing).**

Journal Articles

1. Aparna Viswanathan, "Cyber Law in India: Emerging Trends and Challenges," Journal of Indian Law and Society.
2. Vivek Sood, "Cyber Crime Investigation and Digital Evidence," Indian Journal of Criminology.
3. S. K. Verma & Raman Mittal, "Legal Dimensions of Cybercrime in India," Supreme Court Cases Journal.

Reports and Online Sources

1. Ministry of Home Affairs, Cyber Crime Reports.
2. CERT-In, Annual Reports.
3. Europol, Cybercrime Reports.
4. Law Commission of India, Reports on Criminal Law Reforms