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IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines.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

CYBER CRIMES AND CRIMINAL LIABILITY UNDER THE INFORMATION TECHNOLOGY ACT, 2000: EMERGING LEGAL CHALLENGES

AUTHORED BY - UMANG KAMBOJ

ABSTRACT

The Information Technology Act, 2000 ("IT Act") was India's first, and remains its principal, special legislation criminalising conduct committed through computers, computer networks and communication devices. Enacted to give legal recognition to electronic commerce and subsequently fortified by the Information Technology (Amendment) Act, 2008, the statute today operates as the technical backbone of India's cyber-criminal-liability framework, running in parallel with the Bharatiya Nyaya Sanhita, 2023 ("BNS") and its accompanying procedural and evidentiary codes. This paper undertakes a doctrinal and analytical examination of criminal liability under the IT Act, tracing the statute's legislative evolution from 2000 through the transformative 2008 amendment to its present-day interaction with the Bharatiya Nyaya Sanhita, the Bharatiya Nagarik Suraksha Sanhita, 2023 and the Bharatiya Sakshya Adhiniyam, 2023, which came into force on 1 July 2024. It critically analyses the principal offence provisions — Sections 43, 65, 66, 66B to 66F, 67, 67A to 67C, 69, 69A and 70 — assessing their doctrinal clarity, mens rea requirements, and continuing fitness for purpose against a backdrop of rapidly evolving digital conduct, including ransomware extortion, identity theft, cyberstalking, obscene and sexually explicit content, cyber terrorism, and unauthorised access offences. The paper examines the constitutional and jurisprudential turning point represented by Shreya Singhal v. Union of India, in which the Supreme Court struck down Section 66A for vagueness and overbreadth, alongside subsequent judicial engagement with Sections 66, 66C, 66D, 66E, 67 and 69A in cases addressing identity theft, privacy violation, intermediary liability and content-blocking orders. Employing doctrinal legal research methodology supported by secondary data drawn from National Crime Records Bureau reports and Ministry of Home Affairs disclosures, the paper identifies persistent legal challenges: definitional ambiguity in emergent offence categories such as deepfake-facilitated fraud and artificial-intelligence-enabled impersonation, jurisdictional uncertainty in cross-border digital conduct, intermediary liability tensions under the amended IT Rules, 2021, and the practical difficulty

ISSN: 2582-6433

of reconciling IT Act prosecutions with the newly codified evidentiary regime under the Bharatiya Sakshya Adhiniyam. The paper concludes that while the IT Act remains doctrinally indispensable, its ageing definitional architecture requires targeted legislative refinement, harmonisation with the BNS framework, and institutional capacity-building to remain an effective instrument of criminal liability in India's digital ecosystem.

Keywords: *Information Technology Act, 2000; cybercrime; criminal liability; Section 66A; intermediary liability; electronic evidence; India.*

1. INTRODUCTION

Enacted in the year 2000 to give legal recognition to electronic commerce and to facilitate the filing of electronic records with government agencies, the Information Technology Act, 2000 was, at the moment of its enactment, primarily a commercial-facilitation statute rather than a criminal code.[1] Its criminal provisions were, in their original form, comparatively sparse — confined chiefly to hacking (the erstwhile Section 66) and a handful of offences relating to tampering with computer source documents and unauthorised access. The dramatic expansion of internet penetration in India through the 2000s, and the corresponding proliferation of digitally facilitated fraud, harassment and data theft, rendered this original framework manifestly inadequate, prompting the Information Technology (Amendment) Act, 2008, which substantially rewrote the statute's criminal architecture, introducing the now-familiar suite of provisions from Section 66A through 66F and 67A through 67C.[2]

A quarter of a century after its enactment, the IT Act remains India's principal special statute for cyber-criminal liability, notwithstanding the wholesale replacement of the general penal, procedural and evidentiary codes through the Bharatiya Nyaya Sanhita, 2023 ("BNS"), the Bharatiya Nagarik Suraksha Sanhita, 2023 ("BNSS") and the Bharatiya Sakshya Adhiniyam, 2023 ("BSA"), in force since 1 July 2024.[3] Rather than being subsumed into the new general codes, the IT Act continues to operate as a parallel, specialised statute, and in the overwhelming majority of registered cybercrime cases in India, an accused is charged simultaneously under IT Act provisions and corresponding BNS provisions for the same underlying conduct.[4] This dual-track structure, while functionally necessary given the IT Act's technical specificity,

[1]Statement of Objects and Reasons, Information Technology Act, 2000.
[2]Pavan Duggal, Cyberlaw: The Indian Perspective 58-74 (Universal Law Publishing, 5th edn., 2023).
[3]Ministry of Home Affairs, Notification No. S.O. 1361(E), 24 February 2024.
[4]"Key Provisions Related to Cyber Crimes Under Bharatiya Nyaya Sanhita, 2023 (BNS) – Updated March 2026," LawSection.in.

ISSN: 2582-6433

generates significant doctrinal and practical friction — in classification of offences, in sentencing consistency, and in the coherent development of jurisprudence.

This paper critically examines criminal liability under the IT Act against this evolving backdrop. It asks whether the statute's offence definitions remain sufficiently precise and technologically adaptable to address contemporary digital conduct, how the constitutional check imposed in Shreya Singhal v. Union of India has shaped subsequent legislative and enforcement practice, and what legal challenges — definitional, jurisdictional, evidentiary and institutional — continue to impede the effective attribution of criminal liability for cyber offences in India.[5]

1.1 Statement of the Problem

The IT Act's criminal provisions, though substantially expanded in 2008, were drafted against a technological landscape that predates smartphones, social media platforms, cloud computing, cryptocurrency and generative artificial intelligence in their present form. The consequent definitional gap between statutory text and contemporary digital conduct creates uncertainty in the attribution of criminal liability, generates inconsistent judicial interpretation, and, following the invalidation of Section 66A, has left an identifiable lacuna in the regulation of harmful but non-obscene online expression.

1.2 Objectives of the Study

- To trace the legislative evolution of the IT Act, 2000 from its original enactment through the 2008 amendment to its present interaction with the BNS/BNSS/BSA framework.
- To critically analyse the principal criminal liability provisions of the IT Act, assessing their doctrinal clarity, mens rea structure and practical enforceability.
- To examine the constitutional jurisprudence surrounding Section 66A and its continuing influence on legislative drafting and enforcement practice.
- To identify emerging legal challenges — definitional, jurisdictional, evidentiary and institutional — in the attribution of criminal liability for contemporary cyber offences.
- To propose legislative and institutional reforms to strengthen the coherence and efficacy of criminal liability under the IT Act.

[5]Shreya Singhal v. Union of India, (2015) 5 SCC 1.

ISSN: 2582-6433

1.3 Research Questions

- Do the IT Act's offence definitions retain sufficient doctrinal precision and technological adaptability to address contemporary forms of cyber-enabled crime?
- What is the continuing jurisprudential significance of Shreya Singhal v. Union of India for the drafting and enforcement of cyber-speech offences in India?
- How does the concurrent operation of the IT Act and the BNS affect the coherence, consistency and predictability of criminal liability for cyber offences?
- What legislative and institutional reforms would best address the identified gaps in the IT Act's criminal liability framework?

1.4 Research Methodology

This study adopts a doctrinal legal research methodology, involving critical analysis of the statutory text of the IT Act, its amending legislation, subordinate rules, and judicial precedent, supplemented by secondary literature and descriptive statistical data drawn from National Crime Records Bureau reports and Ministry of Home Affairs parliamentary disclosures. The analysis is confined to India and does not undertake comparative examination of foreign cyber-criminal statutes save where illustrative.

1.5 Scope and Limitations

The paper is confined to the criminal liability provisions of the IT Act (Chapter XI, together with relevant provisions of Chapters IX and XII-A) and their interaction with the BNS framework. It does not address the Act's civil/compensatory provisions in detail (save Section 43, discussed for contrast), sector-specific regulatory penalties, or the substantive content of the Digital Personal Data Protection Act, 2023 beyond its bearing on criminal enforcement. Data cited is the most recent publicly available as of August 2026.

2. LITERATURE REVIEW

2.1 Foundational Commentary on the IT Act

Duggal's early and continuing scholarship on Indian cyber law characterises the IT Act's 2008 amendment as a necessary but imperfect corrective, observing that while the amendment substantially broadened the range of criminalised conduct, it retained a fundamentally reactive, technology-specific drafting style that requires repeated legislative updating to remain current

ISSN: 2582-6433

with evolving digital practice.[6] Kamath's treatment of the pre-amendment IT Act similarly identifies the absence, in the original 2000 statute, of any provision addressing identity theft, phishing or obscene electronic content as a significant early gap subsequently addressed — imperfectly — through the 2008 amendment's introduction of Sections 66C, 66D and 67A.[7]

2.2 The Section 66A Controversy and Its Aftermath

A substantial body of scholarship centres on Section 66A, which criminalised the sending of "grossly offensive," "menacing," or knowingly false information causing "annoyance," "inconvenience," "danger," "obstruction," "insult," "injury," "criminal intimidation," "enmity, hatred or ill will" through a computer resource or communication device.[8] PRS Legislative Research's contemporaneous analysis traces the provision's contested legislative history, including a withdrawn 2013 Private Members' resolution proposing to narrow its scope, and the Supreme Court's interim 2013 order requiring senior police approval prior to any arrest under the section.[9] The Supreme Court's eventual 2015 judgment in Shreya Singhal v. Union of India struck down Section 66A in its entirety as unconstitutionally vague and overbroad, holding that its open-textured language failed to draw a workable distinction between discussion, advocacy and incitement, and consequently had a chilling effect on protected speech under Article 19(1)(a) of the Constitution.[10] Subsequent scholarship documents the troubling persistence of Section 66A prosecutions notwithstanding its invalidation: recent case-law analysis identifies continuing instances between 2022 and 2025 in which police authorities registered complaints or filed charge-sheets under the struck-down provision, prompting renewed Supreme Court directions requiring the purging of the section from police and prosecutorial case-management systems and periodic training of law-enforcement personnel.[11]

2.3 Intermediary Liability and Content Regulation

A distinct strand of literature addresses intermediary liability under Sections 69, 69A and 79 of the IT Act, and the subordinate Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended in 2023. Recent commentary on the 2025

[6]Pavan Duggal, supra note 2, at 95-118.
[7]Nandan Kamath, Law Relating to Computers, Internet and E-Commerce 178-201 (Universal Law Publishing, 4th edn., 2012).
[8]Information Technology Act, 2000, s. 66A (as inserted by the Information Technology (Amendment) Act, 2008) (struck down).
[9]PRS Legislative Research, "A Background to Section 66A of the IT Act, 2000" (2024).
[10]Shreya Singhal v. Union of India, supra note 6, at paras 52-94.
[11]"Latest Judgments Referring to Section 66A of the IT Act," ApniLaw (2025).

ISSN: 2582-6433

amendments to the IT Rules notes the extension of due-diligence and takedown obligations to artificial-intelligence-generated and synthetic content, including deepfakes, read alongside Sections 66C (identity theft), 66D (cheating by personation) and 69A (content-blocking) of the IT Act and complementary BNS provisions criminalising public-mischief-causing misinformation.[12] This literature broadly concludes that while the amended Rules provide MeitY with statutory legitimacy for pre-existing administrative practice regarding deepfake content, the underlying IT Act offence provisions themselves remain unamended and thus continue to rely on analogical extension to synthetic-media conduct.

2.4 Judicial Engagement with Sections 66E, 67 and 67A

Case-law compilations reveal extensive and continuing judicial engagement with Section 66E (violation of privacy through capture, publication or transmission of images of a person's private area without consent) and Sections 67/67A (obscene and sexually explicit material), frequently charged alongside BNS provisions on stalking, voyeurism and outraging modesty, and in cases involving minors, alongside the Protection of Children from Sexual Offences Act, 2012.[13] Bail jurisprudence under Section 483 of the BNSS (successor to Section 439, CrPC) in Section 66E-related matters illustrates the now-routine practice of concurrent charging under IT Act and BNS provisions for the same factual matrix, a pattern this paper examines further in Part 3.[14]

2.5 Statistical and Institutional Literature

NCRB's Crime in India 2024 report documents a 17% year-on-year surge in cybercrime registrations even as overall cognisable crime declined by 6%, a trend independently corroborated in Ministry of Home Affairs parliamentary disclosures noting sustained growth in complaints to the National Cyber Crime Reporting Portal and the 1930 citizen financial-fraud helpline.[15] This literature, read alongside doctrinal commentary on offence-specific provisions, underscores the practical stakes of the definitional and jurisdictional challenges examined in this paper.

[12]"Amendment to IT Rules Regulating AI Generated Content," Lexology (2025).
[13]CaseMine, "Section 66E of IT Act – Indian Case Law" compilation (2026), including Vineesh v. State of Kerala and related bail jurisprudence.
[14]Santosh Patel v. State of Madhya Pradesh, Bail Application, Madhya Pradesh High Court (2025-26), as reported in CaseMine.
[15]National Crime Records Bureau, Crime in India 2024, Ministry of Home Affairs (2026); Lok Sabha Unstarred Question No. 452, Ministry of Home Affairs, answered 2 December 2025.

ISSN: 2582-6433

2.6 Research Gap

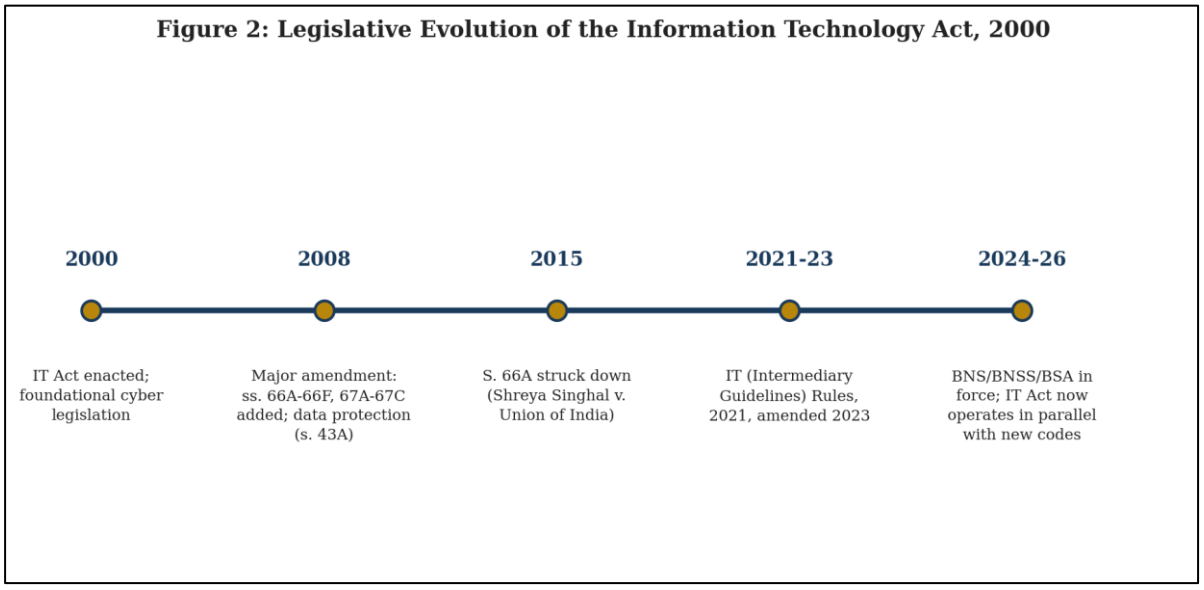
Existing literature tends either to provide provision-by-provision doctrinal commentary on the IT Act in isolation, or to examine the BNS/BSA framework's treatment of cybercrime without close reference to the continuing, structurally central role of specific IT Act offence provisions. This paper integrates both strands, offering an updated (2026) doctrinal account of IT Act criminal liability that is explicitly read against its concurrent operation with the BNS regime, supported by illustrative empirical data.

3. ANALYSIS AND DISCUSSION

3.1 Legislative Evolution of the IT Act

The IT Act's criminal architecture has developed across three distinct phases, summarised in Figure 2. The original 2000 enactment contained a narrow set of offences, chiefly Section 66 (then confined to "hacking" simpliciter) and Section 65 (tampering with computer source documents).[16] The Information Technology (Amendment) Act, 2008 transformed this narrow framework, redefining Section 66 as a broader "computer-related offences" provision cross-referenced to the civil wrongs enumerated in Section 43, and inserting the entire suite of Sections 66A to 66F and 67A to 67C, alongside expanded intermediary and government powers under Sections 69, 69A and 70.[17] The third phase, from 2015 onward, has been shaped by judicial constitutional review (the invalidation of Section 66A) and by the IT Act's altered position within the wider criminal justice architecture following the 2024 commencement of the BNS, BNSS and BSA.

Figure 2: Legislative Evolution of the Information Technology Act, 2000



[16]Information Technology Act, 2000 (as originally enacted), ss. 65-66.
[17]Information Technology (Amendment) Act, 2008 (Act No. 10 of 2009).

ISSN: 2582-6433

3.2 Principal Offence Provisions: A Critical Analysis

3.2.1 Section 43 and Section 66 — Unauthorised Access and Computer-Related Offences

Section 43 enumerates a list of civil wrongs — unauthorised access, downloading, introduction of viruses or contaminants, damage, disruption, denial of access and theft of source code — attracting compensatory liability. Section 66 criminalises the same conduct where committed "dishonestly or fraudulently," importing the mens rea definitions from the erstwhile Indian Penal Code and now, by necessary implication, from the BNS.[18] The maximum punishment under Section 66 is imprisonment up to three years, a fine up to five lakh rupees, or both — a penalty structure scholars have long criticised as disproportionately lenient relative to the scale of harm that sophisticated hacking or data-theft operations can inflict on critical digital infrastructure.[19]

3.2.2 Sections 66B to 66D — Stolen Resources, Identity Theft and Cheating by Personation

Section 66B penalises dishonest receipt of stolen computer resources or communication devices; Section 66C criminalises identity theft — fraudulent or dishonest use of another person's electronic signature, password or unique identification feature; and Section 66D criminalises cheating by personation using a computer resource, a provision of particular contemporary significance given the proliferation of impersonation-based digital fraud, including fraudulent customer-support impersonation, fake investment-platform operators, and — increasingly — AI-voice-cloned impersonation of law-enforcement or judicial officers in so-called "digital arrest" scams.[20] Each of these three provisions carries a maximum sentence of three years' imprisonment and/or a fine up to one lakh rupees (Section 66C) or one lakh rupees (Section 66D), penalty levels that have not been revised since 2008 despite substantial inflation and the escalating financial scale of contemporary identity-theft-facilitated fraud.

3.2.3 Section 66E — Violation of Privacy

Section 66E criminalises the intentional capture, publication or transmission of the image of a person's private area without consent, under circumstances violating that person's reasonable expectation of privacy, carrying a maximum sentence of three years' imprisonment or a fine up to two lakh rupees, or both.[21] Judicial application of this provision has generated a substantial and growing body of case law, frequently charged concurrently with BNS provisions on voyeurism (Section 77) and, in matters involving minors, the Protection of Children from

[18]Information Technology Act, 2000, ss. 43, 66.
[19]Pavan Duggal, supra note 2, at 121-128.
[20]Information Technology Act, 2000, ss. 66B-66D; Lok Sabha Unstarred Question No. 452, supra note 21 (referencing a digital arrest fraud incident of 28 October 2024).
[21]Information Technology Act, 2000, s. 66E.

ISSN: 2582-6433

Sexual Offences Act, 2012.[22] Courts have emphasised that Section 66E requires proof of intent and of circumstances violating a reasonable expectation of privacy, elements that have proved doctrinally significant in bail jurisprudence where the underlying factual matrix is contested.[23]

3.2.4 Section 66F — Cyber Terrorism

Section 66F criminalises acts committed with intent to threaten the unity, integrity, security or sovereignty of India, or to strike terror, through denial of access to computer resources, unauthorised access or penetration attempts, or the introduction of computer contaminants likely to cause death, injury or damage to critical infrastructure, and carries a maximum sentence of imprisonment for life.[24] Despite its severity, reported prosecutions under Section 66F remain rare relative to other IT Act provisions; commentary notes the absence, as of 2026, of any landmark appellate judgment directly interpreting the section's scope, leaving significant interpretive questions — including the provision's application to ransomware attacks against critical infrastructure operators — substantially untested in Indian courts.[25]

3.2.5 Sections 67, 67A, 67B and 67C — Obscene and Sexually Explicit Content

Sections 67 and 67A criminalise the publication or transmission of obscene material and sexually explicit material respectively, the latter carrying a substantially enhanced maximum sentence of five years' imprisonment on first conviction, rising to seven years on subsequent conviction, together with a fine up to ten lakh rupees.[26] Section 67B specifically addresses material depicting children in sexually explicit conduct, carrying enhanced penalties reflecting the particular gravity of child sexual abuse material offences, while Section 67C imposes data-retention and preservation obligations on intermediaries, a provision of direct evidentiary significance for subsequent criminal prosecution.[27]

3.2.6 Sections 69, 69A and 70 — Interception, Blocking and Protected Systems

Section 69 empowers the Central and State Governments to direct interception, monitoring or decryption of information through a computer resource on specified grounds, including the interests of sovereignty, security and public order, while Section 69A empowers content-blocking orders against public access to specified information. Section 70 designates "protected systems" critical to national security or the economy, unauthorised access to which

[22]CaseMine, supra note 12.
[23]Vineesh v. State of Kerala, as reported in CaseMine, supra note 12.
[24]Information Technology Act, 2000, s. 66F.
[25]"Information Technology Act 2000 Section 66F," WorldLawDigest (2026).
[26]Information Technology Act, 2000, s. 67A; "IT Act 2000: Objectives, Features, Amendments, Sections, Offences and Penalties," ClearTax (2026).
[27]Information Technology Act, 2000, ss. 67B-67C.

ISSN: 2582-6433

attracts enhanced imprisonment up to ten years.[28] These provisions, while not primarily criminal-liability provisions in the conventional sense, structure the investigative and preventive apparatus within which cyber-criminal prosecutions under the other sections discussed above are typically initiated.

3.3 The Section 66A Precedent and Its Continuing Significance

The Supreme Court's decision in Shreya Singhal v. Union of India remains the single most consequential judicial pronouncement on IT Act criminal liability. The Court held that Section 66A's key terms — "grossly offensive," "menacing," "annoyance," "inconvenience" and "ill will" — were incapable of objective, judicially manageable application, and that the provision consequently criminalised a substantial quantum of protected speech alongside genuinely harmful communication, rendering it unconstitutionally overbroad and void under Article 19(1)(a) and (2) of the Constitution.[29] The judgment's continuing relevance lies not merely in the invalidation itself but in the interpretive discipline it imposes on subsequent legislative drafting: any future provision criminalising online expression must, to survive constitutional scrutiny, draw a workably precise line between advocacy, discussion and incitement.[30] The BNS's drafters appear to have internalised this discipline, notably declining to introduce an equivalent successor provision, and instead relying on more precisely defined offences — criminal intimidation, defamation, and public-mischief-causing misinformation — to address harmful online expression.

Yet the persistence of Section 66A citations in FIRs and charge-sheets between 2022 and 2025, notwithstanding its 2015 invalidation, illustrates a distinct and troubling enforcement-level challenge: the gap between doctrinal clarity at the appellate level and operational awareness at the level of first-instance policing.[31] The Supreme Court's repeated directions to state governments to purge the provision from police case-management systems and to institute periodic training reflect an acknowledgment that legislative and judicial correction alone cannot guarantee enforcement-level compliance absent sustained institutional follow-through.[32]

[28]Information Technology Act, 2000, ss. 69, 69A, 70.
[29]Shreya Singhal v. Union of India, supra note 6, at paras 78-94.
[30]Id. at paras 83-87 (distinguishing discussion, advocacy and incitement).
[31]ApniLaw, supra note 8.
[32]Id.

ISSN: 2582-6433

3.4 Concurrent Liability under the IT Act and the BNS

As illustrated in Figure 4, the overwhelming majority of registered cybercrime cases in India today involve concurrent charging under IT Act provisions (addressing the technical modality of the offence) and BNS provisions (addressing the underlying general offence — cheating, forgery, criminal intimidation, stalking or organised crime).[33] This structure offers prosecutors valuable flexibility, particularly given the IT Act's comparatively low sentencing ceilings for several key provisions (three years for Sections 66, 66C and 66D), which can be supplemented by the BNS's more severe organised-crime provisions (Sections 111-112) where the conduct forms part of a larger fraud syndicate.[34] However, this same structure generates doctrinal friction: charge-multiplicity disputes over whether cumulative sentencing for the same underlying conduct under both statutes offends the constitutional protection against double jeopardy under Article 20(2); forum ambiguity between courts designated to try IT Act offences and ordinary BNSS criminal courts; and inconsistent classification of offences in official crime statistics, complicating the very empirical assessment this paper undertakes.[35]

3.5 Intermediary Liability and the Regulation of Emerging Content

Sections 69A and 79 of the IT Act, read with the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended in 2023 and further amended in 2025, establish the framework within which intermediaries — social media platforms, internet service providers and hosting services — may claim safe-harbour protection from liability for third-party content, conditional on compliance with due-diligence and takedown obligations.[36] The 2025 amendments extend these obligations to artificial-intelligence-generated and synthetic content, providing statutory legitimacy for MeitY's prior administrative guidance on deepfake content moderation, and operate alongside IT Act identity-theft and personation provisions (Sections 66C, 66D) and BNS provisions on public-mischief-causing misinformation.[37] Nonetheless, no IT Act provision specifically criminalises the creation (as opposed to the malicious use) of deepfake content, leaving the underlying conduct dependent on downstream harm-based offences — a gap this paper addresses further in the Findings below.

[33]LawSection.in, supra note 4.
[34]Bharatiya Nyaya Sanhita, 2023, ss. 111-112.
[35]Kunal Gupta, "Cyber Crime and Digital Evidence Under Bharatiya Nyaya Sanhita (BNS)," 10(1) Iconic Research and Engineering Journals 1-14 (2026), at 4-6.
[36]Lexology, supra note 9.
[37]Id.

ISSN: 2582-6433

3.6 Empirical Dimensions: Sentencing Structure and Prosecution Patterns

Figure 1 depicts the maximum custodial sentences prescribed across the principal IT Act offence provisions, revealing marked disparity: while Section 66F (cyber terrorism) carries a maximum sentence of life imprisonment, the substantially more commonly prosecuted provisions — Sections 66, 66C and 66D, addressing computer-related offences, identity theft and cheating by personation respectively, which collectively underlie the majority of financial cyber-fraud prosecutions — carry a maximum of only three years' imprisonment, a ceiling unrevised since 2008.[38]

Figure 4: Concurrent Liability Structure — IT Act and BNS

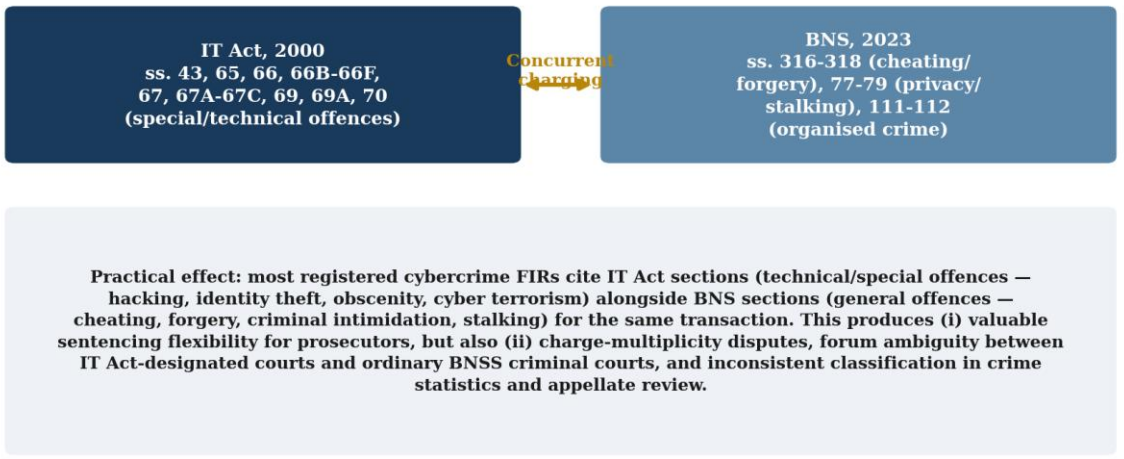
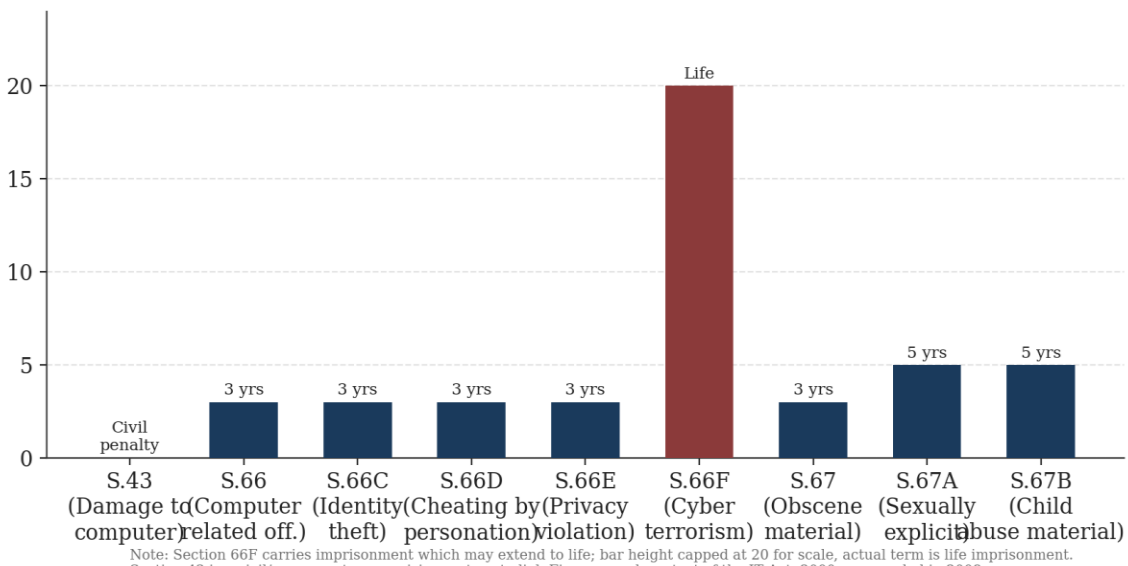


Figure 1: Maximum Custodial Punishment under Key IT Act, 2000 Offence Provisions



Note: Section 66F carries imprisonment which may extend to life; bar height capped at 20 for scale, actual term is life imprisonment. Section 43 is a civil/compensatory provision, not custodial. Figures per bare text of the IT Act, 2000 as amended in 2008.

[38] Information Technology Act, 2000, ss. 66, 66C, 66D, 66F.

ISSN: 2582-6433

Illustrative distribution of prosecutions by offence category, synthesised from NCRB cybercrime case-classification data and secondary legal-practice literature, indicates that fraud and identity-theft-related provisions (Sections 66, 66C, 66D) account for the largest share of registered prosecutions, followed by obscene and sexually explicit content offences (Sections 67, 67A, 67B), with privacy-violation (Section 66E) and cyber-terrorism (Section 66F) charges comparatively rare.[39] This distribution, illustrated in Figure 3, underscores the practical centrality of the identity-theft and personation provisions to contemporary IT Act enforcement, and correspondingly highlights the significance of their comparatively modest sentencing ceilings as a policy concern.

3.7 Emerging Legal Challenges

3.7.1 Artificial Intelligence, Deepfakes and Synthetic Identity Fraud

Neither the IT Act nor the BNS contains a provision specifically defining or criminalising the creation of deepfake content, artificial-intelligence-generated voice cloning, or synthetic identity documents. Prosecutors currently rely on Sections 66C and 66D of the IT Act (identity theft and cheating by personation) and analogous BNS cheating and forgery provisions, an approach that captures the fraudulent use of synthetic media but not its creation or distribution absent proof of a specific fraudulent transaction — a gap of increasing practical significance given the accessibility of consumer-grade generative AI tools.

3.7.2 Jurisdiction and Extraterritorial Application

Section 75 of the IT Act extends the statute's application to offences committed outside India by any person, where the offence involves a computer, computer system or network located in India, a provision of considerable theoretical reach but practically limited enforceability absent effective international cooperation mechanisms. India's continued absence from the Council of Europe's Budapest Convention on Cybercrime, 2001 leaves cross-border evidence-preservation requests dependent on comparatively slower bilateral mutual legal assistance treaty processes, complicating the practical vindication of Section 75's extraterritorial reach.

3.7.3 Encryption, Interception and the Privacy-Security Balance

Section 69's interception and decryption powers must now be read against the constitutional recognition of privacy as a fundamental right in Justice K.S. Puttaswamy v. Union of India, generating a continuing tension between investigative access to encrypted communications and constitutionally protected privacy interests — a tension the IT Act's subordinate rules address

[39]National Crime Records Bureau, supra note 21; Dexpose, "Cyber Crime in India: Statistics, Cases & How to Report" (2026).

 ISSN: 2582-6433

only partially through the traceability obligations imposed on significant social media intermediaries under the amended IT Rules, 2021.

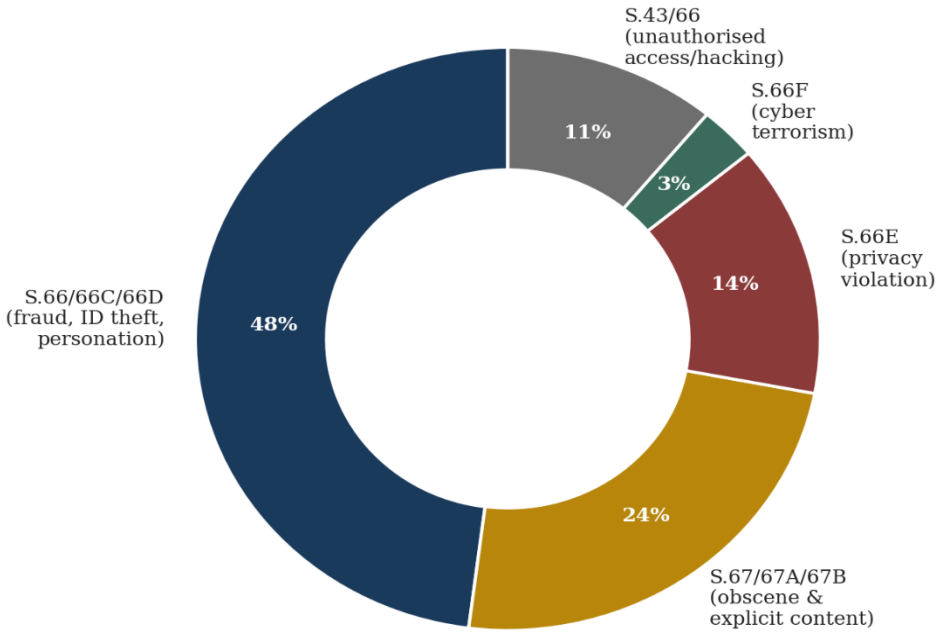
3.7.4 Evidentiary Integration with the Bharatiya Sakshya Adhiniyam

IT Act prosecutions depend critically on the admissibility of electronic evidence — server logs, metadata, device forensic images — now governed by Sections 61 to 63 of the BSA. While the BSA's codified certification regime provides greater doctrinal clarity than the erstwhile Section 65B jurisprudence, practical inconsistency in trial-court application, particularly for evidence held by foreign-headquartered technology platforms, continues to complicate the evidentiary foundation of IT Act prosecutions.

3.7.5 Sentencing Disproportion and Deterrence

The unrevised, 2008-era sentencing ceilings applicable to the IT Act's most commonly prosecuted provisions — Sections 66, 66C and 66D — arguably understate the seriousness of large-scale, syndicate-operated digital fraud, particularly where individual conduct falls short of the BNS's organised-crime threshold under Sections 111-112. This creates a potential deterrence gap for mid-scale fraud operations that are neither petty nor sufficiently organised to attract the BNS's enhanced organised-crime sentencing.

Figure 3: Illustrative Distribution of IT Act Prosecutions by Offence Category



Note: Illustrative distribution synthesised from NCRB cybercrime case-category data and secondary legal-practice literature; fraud/identity-theft-related provisions dominate registered prosecutions.

ISSN: 2582-6433

3.8 Comparative Snapshot: Principal IT Act Offence Provisions

Table 1 below summarises the principal criminal liability provisions examined in this paper.

Provision	Offence	Maximum Punishment
Section 43	Unauthorised access, damage, data theft (civil wrong)	Compensation (civil liability, not custodial)
Section 66	Computer-related offences (dishonest/fraudulent conduct under s. 43)	3 years' imprisonment and/or fine up to ₹5 lakh
Section 66B	Dishonest receipt of stolen computer resource/device	3 years' imprisonment and/or fine up to ₹1 lakh
Section 66C	Identity theft	3 years' imprisonment and fine up to ₹1 lakh
Section 66D	Cheating by personation using computer resource	3 years' imprisonment and fine up to ₹1 lakh
Section 66E	Violation of privacy	3 years' imprisonment or fine up to ₹2 lakh, or both
Section 66F	Cyber terrorism	Imprisonment for life
Section 67	Publishing/transmitting obscene material	3 years' imprisonment (1st conviction); 5 years (subsequent)
Section 67A	Sexually explicit material	5 years' imprisonment (1st conviction); 7 years (subsequent)
Section 67B	Child sexual abuse material	5 years' imprisonment (1st conviction); 7 years (subsequent)
Section 70	Unauthorised access to protected systems	Up to 10 years' imprisonment

Table 1: Comparative snapshot of principal IT Act, 2000 offence provisions and maximum punishment.

ISSN: 2582-6433

4. FINDINGS

- The IT Act's 2008 amendment substantially expanded India's cyber-criminal liability framework, but its offence definitions and sentencing ceilings have not been meaningfully revised since, leaving key fraud-related provisions (Sections 66, 66C, 66D) with comparatively low three-year maximum sentences disproportionate to the scale of contemporary syndicate-operated digital fraud.
- The invalidation of Section 66A in Shreya Singhal v. Union of India established an enduring doctrinal discipline requiring precise, judicially manageable drafting for any provision criminalising online expression, a discipline evidently observed in the BNS's deliberate avoidance of a direct successor provision.
- Notwithstanding its 2015 invalidation, Section 66A continues to be cited in FIRs and charge-sheets as of 2022-2025, revealing a persistent gap between appellate doctrinal clarity and first-instance enforcement-level awareness.
- Concurrent charging under the IT Act and the BNS for the same underlying conduct, while offering prosecutorial flexibility, generates charge-multiplicity disputes, forum ambiguity, and inconsistency in official crime classification and statistics.
- No IT Act or BNS provision specifically defines or criminalises the creation of deepfake content, AI-voice-cloned impersonation, or synthetic identity documents; prosecutions currently depend on downstream harm-based provisions (identity theft, cheating by personation), leaving the creation and distribution of such content itself outside direct criminal sanction absent proof of a specific fraudulent transaction.
- Section 66F (cyber terrorism), despite carrying the Act's most severe penalty, remains judicially under-interpreted, leaving significant questions — including its application to ransomware attacks on critical infrastructure — substantially untested in Indian courts.
- The IT Act's extraterritorial reach under Section 75 remains practically constrained by India's absence from the Budapest Convention framework and continuing reliance on comparatively slow bilateral mutual legal assistance mechanisms.
- Effective IT Act prosecution is increasingly dependent on the evidentiary certification regime under BSA Sections 61-63; while doctrinally clarified relative to the erstwhile Section 65B jurisprudence, practical trial-court application remains inconsistent, particularly for platform-held and cross-border evidence.

ISSN: 2582-6433

5. RECOMMENDATIONS

5.1 Legislative Reforms

- Revise the sentencing ceilings under Sections 66, 66C and 66D to better reflect the contemporary financial scale of digital fraud, potentially introducing graduated, harm-based sentencing tiers linked to quantum of loss.
- Introduce a specifically defined offence addressing the malicious creation and distribution of deepfake content and AI-voice-cloned impersonation, calibrated to avoid the vagueness infirmities identified in Shreya Singhal.
- Clarify, through explicit statutory provision or authoritative judicial guidance, the permissible scope of concurrent charging under the IT Act and the BNS, to reduce charge-multiplicity disputes and forum ambiguity.

5.2 Institutional and Enforcement Reforms

- Institute a mandatory, centrally coordinated system for purging invalidated provisions (such as Section 66A) from police case-management and charge-sheet templates nationwide, with periodic compliance audits.
- Expand specialised judicial and prosecutorial training on the technical elements of IT Act offences, particularly Sections 66E, 66F and 70, to build the interpretive jurisprudence presently lacking for these provisions.
- Strengthen coordination between the Indian Cyber Crime Coordination Centre and state police forces to ensure consistent classification of IT Act versus BNS charges in official crime statistics.

5.3 Evidentiary and Procedural Reforms

- Develop standardised judicial guidance on the certification of cross-border, platform-held electronic evidence under BSA Section 63, to reduce present trial-court inconsistency in IT Act prosecutions.
- Strengthen data-retention and cooperation protocols with intermediaries under Section 67C to improve the timeliness and completeness of evidence available to investigating officers.

5.4 International Cooperation

- Reassess India's position on accession to the Budapest Convention on Cybercrime, 2001, or active engagement with the UN Convention against Cybercrime (2024), to strengthen

ISSN: 2582-6433

the practical enforceability of Section 75's extraterritorial reach.

- Negotiate updated, expedited data-sharing arrangements with major foreign-headquartered technology platforms to support timely IT Act investigations involving cross-border evidence.

6. CONCLUSION

The Information Technology Act, 2000 remains, twenty-six years after its enactment, the doctrinal and technical backbone of India's cyber-criminal liability framework, and its 2008 amendment continues to structure the overwhelming majority of cybercrime prosecutions in the country. Yet this analysis demonstrates that the statute's criminal architecture bears the visible marks of its age: sentencing ceilings unrevised since 2008, offence definitions that do not directly address artificial-intelligence-enabled and synthetic-media conduct, and judicially under-interpreted provisions such as Section 66F whose practical scope remains uncertain. The Supreme Court's landmark intervention in Shreya Singhal v. Union of India stands as an enduring constitutional check on the drafting of cyber-speech offences, yet its incomplete operational absorption at the level of first-instance policing illustrates that judicial correction alone cannot guarantee enforcement-level compliance. The IT Act's continuing concurrent operation alongside the Bharatiya Nyaya Sanhita offers valuable prosecutorial flexibility but equally generates doctrinal friction requiring deliberate legislative and judicial reconciliation. Addressing these challenges will require targeted legislative revision of sentencing structures and offence definitions, sustained institutional investment in specialised judicial and prosecutorial training, strengthened evidentiary protocols attuned to the realities of cross-border digital evidence, and a considered re-evaluation of India's engagement with international cybercrime cooperation frameworks. Only through such integrated reform can the IT Act continue to serve as an effective instrument of criminal liability commensurate with the scale and sophistication of contemporary cyber-enabled crime in India.

REFERENCES

A. Statutes and Legislative Instruments

1. *Information Technology Act, 2000 (Act No. 21 of 2000).*
2. *Information Technology (Amendment) Act, 2008 (Act No. 10 of 2009).*
3. *Bharatiya Nyaya Sanhita, 2023 (Act No. 45 of 2023).*
4. *Bharatiya Nagarik Suraksha Sanhita, 2023 (Act No. 46 of 2023).*

ISSN: 2582-6433

5. *Bharatiya Sakshya Adhiniyam, 2023 (Act No. 47 of 2023).*
6. *Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023).*
7. *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended in 2023 and 2025.*
8. *Constitution of India, arts. 19(1)(a), 19(2), 20(2), 21.*

B. Cases

9. *Shreya Singhal v. Union of India, (2015) 5 SCC 1.*
10. *Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.*
11. *Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.*
12. *Arjun Panditrao Khotkar v. Kailash Kishanrao Gorantyal, (2020) 7 SCC 1.*
13. *Vineesh v. State of Kerala, as reported in CaseMine (2026).*
14. *Santosh Patel v. State of Madhya Pradesh, Bail Application, Madhya Pradesh High Court (2025-26).*

C. Books and Treatises

15. *Pavan Duggal, Cyberlaw: The Indian Perspective (Universal Law Publishing, 5th edn., 2023).*
16. *Nandan Kamath, Law Relating to Computers, Internet and E-Commerce (Universal Law Publishing, 4th edn., 2012).*
17. *S.K. Verma & M. Afzal Wani (eds.), Legal Research and Methodology (Indian Law Institute, 3rd edn., 2013).*

D. Journal Articles and Commentary

18. *Kunal Gupta, "Cyber Crime and Digital Evidence Under Bharatiya Nyaya Sanhita (BNS)," 10(1) Iconic Research and Engineering Journals 1 (2026).*
19. *PRS Legislative Research, "A Background to Section 66A of the IT Act, 2000" (2024).*
20. *"Latest Judgments Referring to Section 66A of the IT Act," ApniLaw (2025).*
21. *"Amendment to IT Rules Regulating AI Generated Content," Lexology (2025).*
22. *"Information Technology Act 2000 Section 66A," WorldLawDigest (2026).*
23. *"Information Technology Act 2000 Section 66F," WorldLawDigest (2026).*
24. *"IT Act 2000: Objectives, Features, Amendments, Sections, Offences and Penalties," ClearTax (2026).*

ISSN: 2582-6433

E. Government Reports and Official Sources

25. *National Crime Records Bureau, Crime in India 2024, Ministry of Home Affairs, Government of India (2026).*
26. *Ministry of Home Affairs, Notification No. S.O. 1361(E), 24 February 2024.*
27. *Lok Sabha Unstarred Question No. 452, Ministry of Home Affairs, answered on 2 December 2025.*

F. Web and Institutional Sources

28. *"Key Provisions Related to Cyber Crimes Under Bharatiya Nyaya Sanhita, 2023 (BNS) – Updated March 2026," LawSection.in, https://lawsection.in.*
29. *"Cyber Crime in India: Statistics, Cases & How to Report," Dexpose (2026), https://www.dexpose.io.*
30. *CaseMine, "Section 66E of IT Act – Indian Case Law" compilation (2026), https://www.casemine.com.*