



Synthetic Deception: Rethinking India's Legal Response to Deepfake-Enabled Fraud

Shravani Dinesh Shinde, Vempaty Bhanu Vamsi, Shivani Agarwal, Pronnati Rajasvi, Sumaiyyah Tasneem, Ashmi Biswas, Pratchi Ghosal, Nayanjita Pathak, Priyanshu Singh, and Atharva Shinde.

ABSTRACT

India is winning the digital revolution but losing the war behind it. Every 24 seconds, a citizen is defrauded online; this caseload far exceeds traditional crimes by orders of magnitude, yet receives only a fraction of legal resources. UPI, mobile banking, and e-commerce are onboarding hundreds of millions of new users, making India the world's largest financial inclusion experiment but also one of the most lucrative testing grounds for scams. India's IT Act, 2000, haphazard BNSS provisions, and reactionary RBI/SEBI directives have proved grossly inadequate to the task of combating cross-border digital fraud involving AI and other emerging technologies. Drawing on National Cyber Crime Reporting Portal data, courtroom precedent, and forensic case studies of phishing syndicates, UPI scams, and ransomware cartels, this study dismantles the myth of legal preparedness. Victims wait years for justice while under-resourced investigators fight twenty-first-century crime with twentieth-century tools. Patchwork amendments are triage, not reform. India urgently requires a dedicated cybercrime code, real-time cross-border enforcement cooperation, and enforceability of the Digital Personal Data Protection Act, 2023. This qualitative doctrinal study applies thematic analysis to legal, regulatory, judicial, policy, institutional, and academic sources. Unlike existing studies, which generally address these issues separately, this study brings together legal, evidentiary, institutional, victim-recovery, intermediary, and cross-border aspects of deepfake-enabled financial fraud. It examines these issues as a connected process, from the identification of enforcement gaps to the reforms needed to address them. Based on these findings, the paper suggests the following: imposing liability for impersonation and synthetic media, strengthening digital evidence mechanisms, improving remedies and victim restitution, increasing intermediary responsibility, and promoting international cooperation.

Keywords: Deepfake; Cybercrime; Fraud; Legal; Digital Evidence; Enforcement; Victims; Vulnerability.



1. INTRODUCTION

The rapid digitisation of financial services and other sectors in India has transformed the way people communicate, transact, access services and perform everyday activities. But the same digitisation has also created new avenues for cybercrime and financial fraud. Cybercriminals are no longer just limiting themselves to old-school methods like hacking and phishing. They are also resorting to using technology and psychological manipulation to impersonate individuals, forge identities and create pressure on victims to part with their money. The scale of the problem can be seen from the financial fraud complaints reported on India's National Cyber Crime Reporting Portal. Between 2021 and 2025, more than 65.89 lakh financial fraud complaints were reported, involving an amount of more than ₹55,050 crore. These figures reflect reported complaints and should not be treated as the complete extent of cybercrime, since not every incident is reported. Within this changing environment, deepfake-enabled fraud has emerged as a particularly difficult form of cyber-enabled deception. Artificial intelligence can now be used to create highly realistic images, videos, and audio that make a person appear to say or do something that never actually happened. In a financial fraud situation, this technology can be combined with impersonation and social engineering. A fraudster may imitate a family member, colleague, senior official, or other trusted person and then create a sense of urgency around a financial transaction. This is important because the victim is not necessarily being deceived because of a lack of digital knowledge. Instead, the fraud may work because the victim believes that the person contacting them is genuine. As synthetic media becomes more convincing, traditional methods of verification, such as recognising a familiar face or voice, become less reliable. The literature reviewed for this study also indicates that factors such as authority, fear, secrecy and urgency can affect a person's ability to stop and verify suspicious communication. The legal problem is equally significant. India already has several laws that can be applied to different forms of cyber-enabled fraud. The Information Technology Act, 2000, contains provisions relating to identity theft, cheating by personation and privacy violations, while the Bharatiya Nyaya Sanhita, 2023, contains provisions that may become relevant depending on the conduct involved. The IT rules and other regulatory measures also place obligations on online intermediaries in relation to unlawful and harmful content. However, neither the BNS nor the IT Act contains a standalone offence which specifically deals with malicious deepfakes/deepfake-enabled financial fraud. Questions are raised regarding not only the absence of the dedicated deepfake offence but also if concepts like "personation" adequately capture AI-generated representations/synthetic identities that are used to mislead victims. Digital arrest scams similarly



have to be dealt with through existing offences, rather than a separate statutory provision. This creates a practical difficulty: the law may provide provisions which can be utilised, but investigators and courts have to determine which provision fits the particular facts of a technology-driven offence. Another difficulty lies with proving what actually happened in the digital space. In a deepfake case, identifying the person who created/circulated the manipulated content may not be straightforward. Investigators may have to establish the source of the material, verify if audio or video has been altered, identify the accounts or devices involved and preserve electronic evidence, which can withstand scrutiny during trial. The involvement of different online platforms, payment intermediaries and service providers can make this process more complicated. The problem becomes even harder where the offender, victim, platform and digital evidence are located in different jurisdictions. Existing research therefore identifies a gap between the speed at which technology develops and the capacity of institutions to investigate, authenticate evidence and recover losses. Victim recovery is another important part of the problem. India has developed mechanisms such as the National Cyber Crime Reporting Portal, the 1930 helpline and the Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS) to facilitate quick reporting and intervention. According to the Ministry of Home Affairs, these mechanisms had helped save more than ₹11,158 crore across over 32.80 lakh complaints by June 2026. However, freezing or preventing the transfer of funds does not automatically mean that the victim receives the money back. The process may involve banks, payment intermediaries, police authorities and courts, making coordination important to the eventual recovery of the amount. Existing research has examined several aspects of cybercrime, including the effectiveness of Indian cyber laws, digital evidence, intermediary accountability, victim vulnerability and law-enforcement challenges. Studies have also considered the growing complexity of financially motivated cybercrime and the difficulties created by offences involving multiple jurisdictions. The gap therefore lies not simply in the absence of a dedicated deepfake offence but in the limited examination of whether existing legal concepts, evidentiary processes and institutional mechanisms can adequately capture the changing forms, scale and consequences of deepfake-enabled financial fraud. There is comparatively less focus on how the legal framework, digital evidence, intermediary responsibility, victim remedies, investigation and cross-border cooperation operate together in cases of deepfake-enabled financial fraud. This study addresses this gap through an integrated analysis of legal, judicial, academic and institutional material. Unlike existing scholarship, which largely examines digital evidence, intermediary liability, victim vulnerability, and enforcement as separate issues, this study



approaches deepfake-enabled fraud as an interconnected enforcement chain spanning prevention and reporting, investigation, prosecution, financial recovery, and international cooperation. Its distinctive contribution is threefold: first, it disaggregates the broad “regulatory gap” into six distinct analytical dimensions, each requiring a corresponding reform lever; second, it identifies a specific doctrinal gap in the application of the concept of “personation” under Section 319 of the Bharatiya Nyaya Sanhita where wholly synthetic personas are used; and third, it moves beyond diagnosis to propose concrete statutory and procedural reforms, including an Interim Digital Restitution Order and upstream watermarking linked to Section 79 safe-harbour protection. It examines the applicability of existing criminal provisions, the interpretation of those provisions in emerging forms of cybercrime, the authentication and attribution of digital evidence, victim protection and financial recovery, intermediary accountability, institutional responses and cross-border enforcement. The study also considers available data and reported cases to understand the difference between having a legal remedy on paper and being able to use that remedy effectively in practice. Based on this analysis, the study identifies areas where legal, regulatory and institutional reforms may be required. It proposes measures concerning AI-based personation, faster mechanisms for financial restitution, clearer intermediary accountability and greater responsibility for generative-AI providers. The broader objective is not simply to create new offences but to examine whether the existing system can respond effectively at each stage of a deepfake-enabled financial fraud, from prevention and reporting to investigation, prosecution, recovery and international cooperation.

2. LITERATURE REVIEW

2.1. Overview

A combination of "deep learning" and "fake", deepfakes are hyper-realistic videos digitally manipulated to depict people saying and doing things that never actually happened. Deepfakes make use of neural networks that employ a set of data samples to enable them to imitate a person’s facial expression, body language, voice, and intonation. ([Westerlund, 2019](#)). With the digitisation of financial systems in developing countries such as India, organised criminals have been taking advantage of these neural networks through cybercrimes. This is a critical issue since attackers are taking advantage of technical loopholes to manipulate human nature and the legal system to extort money through technologies such as deepfakes. This scholarly review dwells on the



interaction between the cyber threat landscape and the victim's psyche and the limitations of the current legal framework to deal with the rising wave of financial frauds. The study focuses on four aspects: rising complex digital frauds, legal framework adequacy, victim vulnerability and the psychology of fraud, and law enforcement, investigations, and victim recovery, to reveal the stark reality of the situation. The review was performed by conducting a search for legal, judicial, and academic literature using terms such as "deepfake", "financial fraud", "IT Act 2000", "BNS", "BSA 2023", "BNSS 2023", "DPDP 2023" and "intermediary liability". The search engines used include Google Scholar, NCRP, ResearchGate, and other governmental sites. The results were extracted using the statutes, relevant Supreme Court and High Court orders, research papers, and reports. Irrelevant or purely technical sources were excluded. The selected material was then examined around the main themes of the study to identify gaps in the legal framework, victim vulnerability, and practical enforcement challenges.

2.2. The Rise of Sophisticated Digital Fraud

Scholars argue that the growing population, particularly amid widespread digitisation, has substantially transformed criminal activities. These activities have evolved from isolated software breaches into organised, transnational service economies and increasingly sophisticated forms of psychological manipulation. The Liferac model shows that the problem of cybercrime is complicated by the fact that evidence is often disappearing as the cyber activity is happening and needs to be captured in a timely manner. (Grobler, Solms, 2009) The limitless nature of cyberspace compounds this challenge, as networks connected through the internet can share information instantly across geographic distances, with physical isolation being the sole limiting factor. (Subair et al., 2022) The authors concluded that the increased use of e-commerce and online transactions presents significantly greater exposure to the risk of cybercrime. The threat of AI-fuelled cyberattacks is increasing with the ability of criminals to deploy targeted phishing schemes and evasive malware like Lumma Stealer to steal financial data. Data analysis shows that malware such as Infostealer and RedLine has already compromised tens of thousands of computers, stealing payment data and credentials. Researchers note that telecom fraud and identity theft – including SIM swapping and abuse of Aadhaar – also facilitate the improper diversion of funds. Cyber-enabled financial crime is targeting not only computer data but also identity, authentication, and trust relationships in digital transactions. Thus, impersonation emerges as an important link between technological and financial fraud. Information security analysts noted that



telecommunications and identity theft frauds, such as SIM swapping, are being used to circumvent traditional telecommunication safeguards. Impersonation therefore becomes an important link between technological capability and financial deception. Moreover, security analysts emphasise that attackers are exploiting weaknesses in telecommunications and identity-verification frameworks, including SIM swap fraud, while systematically circumventing conventional security boundaries. Overall, recent scholarship suggests that these operations are increasingly directed by globalised organised crime syndicates, thereby complicating cross-border enforcement and digital forensic investigations. (ICT Cyber Desk, 2016). As deception moves from compromising systems towards manipulating identities and trusted communications, it raises the question of whether conventional concepts of identity theft, cheating and personation can adequately address technologically mediated impersonation. This provides the basis for examining deepfake-enabled fraud and digital arrest scams in the next theme.

2.3. Adequacy of the Existing Legal Framework

Within this evolving cybercrime environment, digital arrest scams and deepfakes have emerged as newer forms of cyber-enabled fraud, facilitated by advances in artificial intelligence and digital communication. (Arctic Wolf, 2024) Digital arrest is frequently mistaken for a legitimate law enforcement procedure; however, it refers to fraud in which criminals impersonate police officers or government officials through fake documents and threaten victims with arrest, account freezing, or passport cancellation unless payment is made. Deepfakes constitute highly realistic AI-generated media that employ an individual's face or voice to make them appear to say or do things they have never done, often without consent. Depending on the conduct involved, such offences may be addressed through existing provisions of the Bharatiya Nyaya Sanhita, 2023 (BNS) and the Information Technology Act, 2000 (IT Act). (Singh, 2024) Under the BNS, Section 351 addresses criminal intimidation, Section 356 addresses defamation, Section 75 addresses sexual harassment, Section 77 addresses voyeurism, and Section 79 addresses words, gestures, or acts intended to insult the modesty of a woman. Under the IT Act, Section 66C addresses identity theft, Section 66D addresses cheating by personation using a computer resource, and Section 66E addresses violations involving privacy of private areas, while Sections 67 and 67A address electronic publication or transmission of obscene and sexually explicit material. NCRB data show that cases registered under Section 66C increased from 784 in 2014 to 1,081 in 2015, while Section 66D cases rose from 428 in 2014 to 1,083 in



2015 and 1,597 in 2016. Although Section 66D data continued to be reported at the State/UT level through 2019, comparable recent nationwide figures specifically disaggregated by Sections 66C and 66D were not identified, limiting assessment of their current enforcement and conviction outcomes. (Ministry of Home Affairs, 2026) However, neither the BNS nor the IT Act contains a standalone offence specifically targeting malicious deepfakes. Likewise, digital arrest scams are tackled with existing offences, rather than a specific statutory provision. This creates challenges in terms of attribution, digital evidence verification and the application of legal penalties. This raises a broader question of whether legal concepts of conventional deception fully capture synthetic identities and digitally created representations. In cases of AI-enabled personification, establishing deception also requires identifying who or what is being impersonated and how the synthetic representation should be legally characterised. The problem also extends to evidence: proving that content was manipulated does not necessarily establish who created or used it for fraud. Authentication, provenance and attribution are therefore important to the application of existing offences. These legal and evidentiary questions are linked closely to the victim's perception of authenticity, especially where the impersonation invokes authority, familiarity, fear, or urgency.

2.4. Victim Vulnerability and the Psychology of Fraud

Beyond these challenges, deepfake-enabled financial fraud arises not from victim ignorance but from the exploitation of trust and urgency, as the reliability of visual verification declines (Borwell, Jansen, & Stol, 2022). As synthetic audio and visual content become realistic, traditional cues such as familiar faces and voices become less reliable, challenging the assumption that "seeing is believing". Some researchers identify emotional and financial harm, as well as barriers to reporting, and introduce a vulnerability-peak model (Zhang, Xian, & Schaub, 2025). This model suggests that susceptibility is highest within intermediate relationships, such as colleagues, superiors, and familiar professionals, who may be impersonated in fund-transfer fraud. Deepfakes can enhance such social-engineering attacks with the aid of familiar identities, as well as the pressures and secrecy. In this manner, the fear and perceived authority can interfere with verification, override reasoning and create cognitive overload, leaving digitally literate individuals vulnerable. Susceptibility is more closely associated with impulsivity and cognitive style than to age or education (Dadà et al., 2025), and scam awareness rarely encompasses deepfake-specific risks (Mehta, Patil, & Meghani,



2025). These findings suggest that victim vulnerability is not solely a matter of awareness or digital literacy but is influenced by the context of the financial decisions. This has implications beyond the moment of the fraud because the psychological pressure can also impact the victim's ability to acknowledge the deception, report it in a timely manner, and recover. Industry data indicate anxiety, betrayal trauma, and diminished confidence in safeguards such as video call verification. RBI data report over 10,000 institutional fraud cases totalling ₹48,000 crore in FY26. Because deepfake scams involve low production costs and high rewards, these incentives push criminals towards scalable, authority-based impersonation at an "industrial scale", leveraging institutional trust rather than building credibility (Shamo, 2025). The impact of harm is uneven: while urban victims may absorb losses, similar losses can be catastrophic for low-income or rural households, reinforcing the need for victim-differentiated research (Paramasivan et al., 2026). The literature therefore establishes vulnerability and harm but provides less integrated analysis of how these factors connect with reporting, financial recovery and institutional support. Once victims report or attempt to recover losses, the effectiveness of the response depends on enforcement capacity, coordination and available mechanisms for redressal, leading to the next theme.

2.5. Law Enforcement, Investigation, and Victim Recovery

The literature identifies a persistent gap between the rapid development of cybercrime and the institutional capacity available to investigate and respond to it (Wall, 2007). Enforcing laws against digital fraud is inherently complex due to jurisdictional fragmentation, where cross-platform and multi-account schemes fall under the overlapping duties of separate, often under-resourced agencies with inconsistent evidence-handling standards (Brenner, 2006; Hunton, 2011). These systemic hurdles are intensified in deepfake-driven fraud cases, where proving content manipulation is merely the initial step because investigators must further trace the media's origin, link it directly to the financial loss, and definitively identify the perpetrator. Victim recovery presents a related but distinct institutional challenge. Literature highlights secondary victimisation through institutional indifference, victim liability, and the absence of standardised compensation mechanisms (Button et al., 2014). This indicates that the existence of reporting and financial-fraud intervention mechanisms does not necessarily demonstrate effective victim redressal. Reporting, freezing or tracing funds, investigation, prosecution and recovery are separate stages that require coordination among police, banks, platforms and other institutions, yet they are not consistently examined as one process. Existing provisions



such as Sections 66C and 66D of the IT Act may be invoked in appropriate cases involving emerging digital fraud, although their application raises questions of legal fit and interpretation (Duggal, 2021). The literature highlights several separate yet interrelated obstacles: limited enforcement capacity, inconsistent handling of digital evidence, poor institutional coordination, and inadequate victim recovery. Separating these issues is crucial because each demands a specific solution such as legal reforms, expanded investigative resources, standardised procedural tools, or stronger inter-agency cooperation rather than being misdiagnosed as a single, uniform regulatory flaw.

2.6. Summary

Recent research has revealed that cybercrime is no longer reliant on isolated technical devices but rather an organised business. The researchers note the involvement of synthetic media in the commission of the crime, which challenges the eye, and the cognitive biases of the victim. Although the literature provides explanations about the mechanism involved in the creation of confusion, researchers are now more concerned with the delay in legislative adjustments to cybercrimes. The evidence shows that authorities are stretching existing laws to cover new types of crimes. At this juncture, it becomes apparent that the researchers reveal the existence of a capability gap in the current crime prevention framework. Technology-facilitated crimes are far ahead of the investigative and recovery capabilities of the current legal system.

2.7. RESEARCH GAP:

Policy reform suggestions for enhancing India's existing legal framework on deepfake-enabled fraud

Existing literature identifies Indian legal provisions addressing certain forms of digital and deepfake-enabled fraud, but researchers encounter difficulties applying them to emerging technology, digital evidence, intermediary liability, enforcement, victim vulnerability, and cross-border investigation. The reviewed literature establishes that India lacks explicit provisions specifically addressing deepfake-enabled fraud, while the inadequacy of existing laws, delays in cross-border cooperation, and the safe-harbour framework under Section 79 create uncertainty regarding intermediary accountability. Researchers differ on the extent to which the 2026 IT Rules address these gaps completely as a progressive legal step to fill these gaps.



Furthermore, there are differing views on the effectiveness of compensation arrangements for victims and whether safe harbour enhances the platform's duty to remove SGI voluntarily. Compared to jurisdictions such as the European Union and China, the requirements for synthetic media are less specific in New Zealand, for example, by not being codified as a requirement for disclosure or labelling, or as a requirement for machine-readable labelling, as in the case of the EU, or as a requirement for provider-level verification, content review, traceability, and labelling, as in China ([Eswaramoorthi, 2026](#)). India's recent signing of the United Nations Convention against Cybercrime further demonstrates its commitment to strengthening international cooperation in combating cybercrime and facilitating the sharing of electronic evidence across jurisdictions. ([United Nations, n.d.](#)) These developments suggest that India could further strengthen its framework by establishing more mechanisms to enhance transparency and traceability while providing some clarity regarding the intermediary's role in detection and response to fraud using deepfakes. ([DD India, 2026](#)).

Statutory design, enforcement resources, and coordination gaps are mixed in with existing scholarship under "regulatory gaps". Legislation, budget/capacity, and protocols are needed for statutory, resource, and coordination gaps, respectively. Disaggregation is essential to provide the information needed to make recommendations that can inform actionable reforms and inform policymakers what levers to prioritise. Our research examines six aspects: legal coherence, digital evidence authentication, intermediary liability, enforcement, victim remedy, and cross-border cooperation. It recommends specific laws for SGI-induced financial frauds, capacity building for forensic and prosecution institutions, proactive mechanisms against deepfake-enabled fraud, and cross-border agency coordination. The unique value of this research is that it adopts an 'end to end' approach to the enforcement of deepfake-related crimes, as opposed to merely focussing on the legal, evidentiary and recovery aspects of a crime, and that it proposes practical statutory and procedural changes to address deepfake-related crimes by applying the six dimensions analysis, rather than simply introducing the absence of a specific offence relating to deepfakes.

3. RESEARCH METHODOLOGY

3.1. Research design

This study uses a qualitative doctrinal approach with thematic analysis to examine the adequacy of India's legal and regulatory framework in addressing cybercrime and digital fraud, with particular focus on emerging



threats such as deepfakes and digital-arrest scams. The research examines the subject through four broad areas: technological developments in cybercrime, the Indian legal framework, victim vulnerability, and law enforcement and financial recovery. Relevant laws, regulations, institutional mechanisms, judicial decisions, and scholarly research are examined within these areas to understand how the existing framework responds to emerging forms of digital fraud. Thematic analysis is used to organise and compare these materials across the four areas and to identify recurring legal, evidentiary, institutional, and enforcement issues. The study also considers weaknesses in the present framework and identifies aspects where changes in law, enforcement, or institutional practices may be needed.

3.2. Nature of research

The selected research design is used to analyse existing laws, research papers, legal provisions, and other scholarly materials, and does not involve conducting surveys or interviews. The qualitative approach facilitates an understanding of the nature and impact of cybercrime and deepfake-enabled fraud through systematic analysis of existing information. The doctrinal and analytical nature of the research allows legal provisions and institutional mechanisms to be examined in relation to the emerging forms of fraud discussed in the study, while thematic analysis facilitates comparison across the identified areas of inquiry. It is also supported by descriptive secondary statistics from institutional reports, used to indicate the scale of the problem rather than for statistical testing. These statistics are therefore used to provide contextual evidence on the reported scale of cybercrime and financial fraud, rather than to establish causal or statistical relationships. Also, the research evaluates the adequacy of existing laws and identifies gaps requiring further development.

3.3. Sample and its technique

The study does not involve a human or survey-based sample. Instead, its documentary sample comprises academic research papers, legislation and regulations, judicial decisions, government and institutional reports, policy materials, and selected international legal and regulatory sources relevant to cybercrime and digital fraud.

Sources were selected through purposive sampling using four principal criteria:

- (i) direct relevance to the research questions and six analytical dimensions;



- (ii) substantive discussion of cybercrime, digital fraud, deepfakes, digital evidence, victim vulnerability, intermediary responsibility, enforcement, financial recovery or cross-border cooperation;
- (iii) credibility and traceability of the source;
- (iv) relevance to the Indian legal and institutional context, with international sources included where comparative analysis was required.

Recent sources were prioritised for emerging technologies and regulatory developments, while foundational studies were retained where they provided established theoretical, legal or forensic perspectives. Sources were excluded where they were primarily opinion-based, lacked sufficient methodological or bibliographic information, were not directly relevant to the research questions, or duplicated evidence already represented by a more authoritative source. Primary legal and institutional materials were prioritised for statements concerning legislation, regulations, government mechanisms and official statistics, while peer-reviewed and scholarly sources were used to develop the conceptual and analytical framework. This selection approach ensures that the documentary sample is sufficiently focused to address the study's research gap while retaining different forms of evidence necessary for analysing legal, evidentiary, institutional and victim-related dimensions.

3.4. Data collection tool

The study used a structured review of documentary sources as the principal method for collecting the material required for the study. Published academic research papers on cybercrime, digital fraud, cybersecurity, and cyber laws in India were identified primarily through Google Scholar. These were supplemented by relevant legislation, regulations, judicial decisions, government and institutional reports, and selected international materials. The materials were identified and selected according to their relevance to the four main themes of the study: technological developments in cybercrime, the Indian legal framework, victim vulnerability, and law enforcement and financial recovery. The selected sources were then reviewed thematically to identify legal issues, gaps, enforcement challenges, and areas of disagreement across the literature and legal framework.



3.5. Variables used

Since this is a doctrinal and qualitative study, “variables” are understood as key legal concepts and analytical dimensions rather than quantitative measures. The analysis focuses on the legal and institutional response to cybercrime and digital fraud. Relevant statutory provisions, judicial decisions, policy materials, and scholarly literature were organised and examined under six analytical dimensions to identify gaps, ambiguities, and enforcement challenges in the existing framework. These dimensions are:

1. Availability and applicability of criminal laws and mechanisms for prosecution.
2. Interpretation and applicability of existing laws to emerging forms of cybercrime.
3. Victim protection, compensation, financial recovery, and redressal.
4. Intermediary liability and accountability.
5. Roles and challenges of investigators, prosecutors, and courts in cybercrime enforcement.
6. Cross-border jurisdiction and mechanisms for international cooperation and enforcement.

3.6. Ethical consideration

This study is conducted only using publicly available legal texts, government reports, and published scholarship. It involves no primary human participants or personally identifiable data. All statistics and case references are attributed to their original sources with accurate citations. As deepfake fraud is a sensitive subject, the study avoids unnecessary disclosure of personal information when discussing reported cases.

3.7. Limitations

The findings of the study should be considered in light of its qualitative doctrinal approach and its dependence on secondary legal, institutional, and academic sources. While doctrinal research is useful for examining the content and development of law, it cannot by itself show how legal provisions operate in actual cases. Consequently, the study cannot independently assess the effectiveness of these provisions at different stages of cybercrime proceedings, including investigation, registration of cases, forensic examination, prosecution, trial, and conviction. Institutional statistics are also generally based on reported incidents and may not reflect the full extent of cybercrime, as some victims may choose not to report their experiences because of stigma, embarrassment, or other concerns. In [X v. Union of India \(2023\)](#), the Delhi High Court has recognised the



potential for the injury to the victim in the event of intimate images being posted on the internet without his consent and has directed the prompt removal, de-indexing and protection of his identity as well. This applies to deepfakes involving sexual images. The absence of primary interviews with victims and enforcement personnel further limits the study's ability to capture experiences at the operational level. In addition, the purposive selection of sources may mean that some judicial or regional developments are not represented. Finally, changes in the regulatory framework, particularly the 2026 IT Rules, may influence the continuing relevance of the findings.

4. DATA ANALYSIS

4.1. Introduction

This section analyses the legal, scholarly and institutional material collected for the study to examine how India's existing framework responds to cybercrime and emerging forms of digital fraud, particularly deepfake-enabled fraud and digital-arrest scams. The study considers provisions under the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Information Technology Rules and the Digital Personal Data Protection Act, 2023. Judicial decisions, research papers and institutional reports have also been considered. Along with the legal provisions, the section looks at reported cybercrime and financial-fraud data and the difficulties that arise in investigation, handling electronic evidence, recovering victims' losses, dealing with intermediaries and addressing crimes that cross national borders. The main focus is to see whether the existing legal provisions can be applied to newer forms of cybercrime and where difficulties or gaps arise in doing so.

4.2. Data Overview/Sample Profile

The material analysed for this study mainly consists of existing legal, academic and institutional sources on cybercrime and digital fraud in India. These include laws and regulations, judicial decisions, research papers, scholarly articles and reports from government and other institutions. The material covers the existing legal position as well as reported trends in cybercrime and financial fraud, with a focus on newer issues such as deepfakes and digital-arrest scams. It also covers areas such as victim protection, investigation, electronic evidence, intermediary responsibility, financial recovery



and cross-border enforcement. Since the study is based on existing sources, it does not capture the experiences of every victim or the actual extent of cybercrime in India. Instead, the material gives an overview of how the present legal and institutional framework deals with these forms of cybercrime and where difficulties can be seen.

4.3. Descriptive Analysis

The material reviewed shows that cybercrime in India is becoming more difficult to deal with as the methods used by fraudsters continue to change. Deepfakes, fake identities and manipulated audio and video can make a fraudulent communication appear genuine. Because of this, identifying the person responsible is not always straightforward. It can also be difficult to establish whether the digital evidence available in a case is authentic and can be relied upon.

The material also shows that the problems do not end once a victim reports the fraud. In many cases, the victim has to deal with the loss of money as well as the difficulty of getting it back. Investigation may require digital forensic analysis and cooperation between different authorities. This becomes harder when the relevant evidence is held by an online platform or when the people involved are located outside India. A common issue across the material is also the overlap between different areas of law. A single incident may involve cheating or impersonation, the use of computer resources, data protection issues, platform obligations and financial transactions. As a result, one provision may not be enough to deal with the entire incident. The same problem can become more complicated when synthetic content is involved because it may be difficult to determine who created it, who shared it and who should be legally responsible.

The overall picture is therefore more complicated than simply asking whether India has laws against cybercrime. The existing laws can cover different parts of a cybercrime or fraud case, but applying them to newer forms of fraud can raise questions about evidence, identification of the offender, responsibility of intermediaries and recovery of the victim's money.

4.4. Distribution of Legal Provisions Applicable to Deepfake-Enabled Fraud

Table 1 shows that offences of deepfake and 'digital-arrest' fraud are not confined to any specific Indian response. If the BNS and IT Act can be used together, the investigators must prove the elements of identity misuse, deceptive intent, intimidation, or transmission of illegal material. This poses a huge enforcement



problem if the synthetic audio or video is very realistic, anonymously published, produced outside of India, or gets reposted quickly on various platforms.

Table 1: Legal Provisions Applicable to Deepfake-Enabled Fraud

Fraud scenario	Legal provisions	Enforcement and practical implications
Financial fraud using deepfake impersonation	BNS provisions on intimidation, cheating, forgery, and conspiracy; IT Act S.66C and S.66D	The authorities have to prove that the accused was aware of the impersonation of another person and that he/she was trying to mislead. Determining creators, maintaining metadata, tracking financial flows, and obtaining platform evidence can be a time delay. (Miglani & Parihar, n.d.)
Non-consensual intimate deepfakes	BNS S.75, 77, and 79; IT Act S.66E, 67, and 67A	This is comparatively more actionable since provisions on privacy, sexual harassment, voyeurism, and obscenity are more focused on identifiable harms. Yet, quick takedown, survivor protection, and cross-platform removal are still challenges.
Digital-arrest scams	BNS S.351 and general cheating provisions; IT Act S.66D	Current regulations deal with impersonation and intimidation but are not specific to the coercive nature of a fake online arrest. Victims can transfer money prior to verification systems in place.



Corporate government impersonation	or General cheating, forgery, conspiracy; IT Act S.66C and S.66D	Judicial rulings determine liability based on the question of “personation” in the context of synthetic identities. In cases involving corporate targets, the evidentiary burden of relying on and suffering a financial loss is obvious, as is the burden of attribution.
------------------------------------	--	--

It is, therefore, crucial that the judiciary interpret it. Personification and cheating laws may be expanded to synthetic media, but there is the potential for confusion regarding their application from police, platforms, and victims. Without a specific deepfake crime, enforcement is likely to be inconsistent, and a more precise definition of the crime, faster evidence preservation, and platform accountability measures are needed.

4.5. Variable-wise/Analytical Dimension Analysis

4.5.1. Availability and Applicability of Criminal Laws and Mechanisms for Prosecution

The legal framework dealing with cybercrime involves provisions under both the Information Technology Act, 2000, and the Bharatiya Nyaya Sanhita, 2023. Some offences under the IT Act specifically deal with the use of technology, while similar forms of conduct may also be dealt with under the BNS. This overlap can make it difficult to decide which provision should be applied in a particular case. The issue becomes more important when the conduct does not fit neatly into one category of offence. Investigation can also become difficult where the offence involves different jurisdictions or digital platforms. Cheating implies the element of fraudulent or dishonest inducement in addition to deception, as the Supreme Court had stated in [Hridaya Ranjan Prasad Verma v State of Bihar](#), in cases where the impersonator lures the target to send money, claiming to be a police officer, a judge or any other public officer. While investigating cyber-fraud cases, the Supreme Court in [S.W. Palanikar v. State of Bihar](#) has clarified that criminal cheating is an offence of dishonest intention at the time of the representation, and the investigators must find more than just a fact of the victim having suffered financial loss. Section 78 of the IT Act further provides a specific framework regarding the officers who can investigate offences under the Act. Overall, the material suggests that the



difficulty is not simply a lack of legal provisions but also the need to apply different provisions consistently to the facts of a cybercrime case.

4.5.2. Interpretation of existing laws for deepfake-related frauds

Bharatiya Nyaya Sanhita, 2023 (BNS), and the Information Technology Act, 2000 (IT Act), do not address frauds organised utilising deepfake technology explicitly. ([Chaitanya Rohilla v. Union of India, 2023](#)) For this, courts are forced to interpret the sections with generic fraud definitions that are drafted for a completely different use case, not for AI-generated harms. (Chauhan, 2026) (["Calcutta High Court transfers", 2026](#)) This may result in open interpretation of sections that could cause significant delay in enforcement and justice.

Table 2: Current statutes and capability gap

Current statutes	Insufficiency argument	Judicial Interpretation & Enforcement Reality
Section 336 of the BNS Act (forgery)	May hold the human using AI accountable; no liability for the intermediary.	Judicial Friction: Courts traditionally require a false document to be made with deceptive intent. Applying physical forgery jurisprudence to algorithmically generated pixels leads to quick quashing petitions by defence teams.



Section 319 of the BNS Act (cheating by impersonation)	Targets financial fraud; alternative remedies are less efficient for the humiliation and reputational loss caused by deepfakes.	Statutory Loophole: Indian jurisprudence for impersonation requires assuming the identity of a specific, existing person. Syndicates deploying entirely synthetic AI personas routinely exploit this to avoid S.319 framing.
--	---	--

Source: Authors' analysis of current statutes

4.5.3. Victim Protection, Compensation, Financial Recovery and Redressal

The material shows that dealing with a cybercrime complaint involves several stages, beginning with reporting and investigation and potentially extending to tracing the funds and obtaining compensation or other forms of redress. In [State Bank of India v Pallabh Bhowmick](#), the Supreme Court has confirmed that a bank is not entitled to pass the onus of an unauthorised electronic transaction onto its customer unless it makes a satisfactory finding of the relevant facts, which include any alleged customer negligence. The effectiveness of the process will depend on the speed of reporting the problem and the extent to which the involved agencies cooperate with each other. The problem can also become complex if electronic evidence needs to be obtained from various platforms or authorities. Although there are restitution and compensation laws, their presence cannot guarantee that the victim will recover the losses they underwent. In practice, the speed of reporting, tracing and coordination between agencies can have an important bearing on the outcome.

4.5.4. Intermediary liability and accountability

Table 3: Liability. Current statutes and capability gap



Current statutes	Insufficiency argument	Practical Implication and Enforcement Gap
Section 79 of the IT Act 2000	Intermediaries can act as neutral hosts under a conditional safe harbour and have limited liability.	Reactive Shield: Safe harbour relies on notice-and-takedown. By the time a judicial or executive order forces removal, the fraud is complete and funds have exited the jurisdiction, making the immunity shield detrimental to proactive fraud prevention.
Rule 2(1)(wa) & Rule 4 Mandates of IT Amendment Rules.	Synthetic media generated using open-source models may not contain metadata.	Forensic Dead End: Without mandatory upstream cryptographic watermarking like C2PA embedded at the point of generation, investigating officers cannot authenticate origin, rendering traceability mandates practically unenforceable in court.

Source: Authors' analysis of current statutes

The Supreme Court, in [Shreya Singhal v Union of India](#), reiterated the conditional safe harbour of Section 79 of the Information Technology Act with a narrow interpretation of “actual knowledge”, which struck a



balance between the rights of the platform to protect its platform, the rights of due process, and the rights to speedily remove unlawful deepfake content.

The analysis indicates that Section 79 provides a safe harbour for companies, given that companies enforce takedown measures and maintain compliance. (*X v. State [NCT of Delhi]*, 2026) The IT Amendment rules 2026 also require platforms to take proactive, automated measures. Despite this, the framework remains unclear when the content evades detection, creating accountability issues. (*Parliament of India, Committee on Empowerment of Women*, 2026)

4.5.5. Investigators, Prosecutors and Courts: Enforcement Gap

India has substantive provisions under the IT Act 2000 (66C & 66D), alongside BNS 2023 (Sec 318 & 319), while BSA 2023 (Sec 61–63) provides a framework for electronic evidence.

From 2021 to 2025, over 65.89 lakh financial fraud complaints involving more than ₹55,050 crores were reported, while over 1.98 lakh FIRs were registered.

In *Anvar P. V. v. P. K. Basheer*, the SC stated that in the era of deepfakes, the authentication of content on the platform, chat logs, audio recordings, video footage, and call history will be crucial and that secondary electronic records (SECRs) will have to meet the statutory requirements to be accepted as evidence (*Anvar P. V. v. P. K. Basheer*, 2014). In its *Arjun Panditrao Khotkar vs. In the Kailash Kushanrao Gorantyal* judgement, the Supreme Court restated that in general, a certificate is required for secondary electronic evidence, pointing out the difficulties in proving that manipulated or AI-generated evidence is reliable, complete and originated from a specific source (*Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, 2020).

In *Tomaso Bruno v. State of Uttar Pradesh*, the Supreme Court reiterated the need for the preservation of the possession of the best evidence in electronic form and held that preservation of the devices, server logs, metadata, CCTV footage, transaction trail and records of the platform were necessary for investigations relating to cyber-fraud (*Tomaso Bruno v. State of Uttar Pradesh*, 2015).

Although India has several laws and a wide reporting system for cybercrime, the available data does not clearly show how many complaints actually move from investigation and forensic examination to prosecution, trial, and finally conviction.



The changing nature of fraud, particularly deepfakes, accentuates this challenge by making attribution, authentication and preservation of digital evidence increasingly complex. Moreover, available data does not separate deepfake fraud from general digital fraud, limiting assessment of its specific enforcement burden.

4.5.6. Cross-border Jurisdiction and International Cooperation

Cybercrime increasingly creates cross-border jurisdictional challenges, as perpetrators, victims, digital evidence, platforms and financial proceeds may be located in different countries. Evidence can disappear much faster than formal legal cooperation operates. India has established mechanisms, including MLATs and bilateral cooperation agreements with 40 countries, while I4C coordinates international cooperation relating to cybercrime. However, the effectiveness and speed of these mechanisms remain concerns. A 2025 Parliamentary Committee identified prolonged MLAT and Letters Rogatory timelines and difficulties in obtaining data from foreign service providers as significant obstacles to investigation. A 2026 FIU-IND case further illustrates the scale, involving ₹868 crore, 5,000+ mule accounts and cryptocurrency transactions across multiple jurisdictions. Yet, national cybercrime statistics do not separately quantify cross-border cases, making the extent of this enforcement gap difficult to measure.

4.6. Statistical/Documentary Findings

The data available on cybercrime in India shows a clear rise in the number of complaints being reported. As per Ministry of Home Affairs data, cybercrime incidents registered on the National Cyber Crime Reporting Portal (NCRP) increased from 452,429 in 2021 to 2,268,346 in 2024. This amounts to an increase of around 401%. These numbers refer to incidents reported through the NCRP and should not be confused with FIRs, prosecutions or convictions. Financial fraud has followed a similar pattern. Financial-fraud complaints increased from 262,846 in 2021 to 2,402,579 in 2025, which is an increase of about 814%. At the same time, the reported financial loss went up from ₹551 crore to around ₹22,495 crore. The rise in losses is much larger than the rise in the number of complaints. When the total reported loss is divided by the number of complaints, the average reported loss comes to about ₹20,963 per complaint in 2021, compared with approximately ₹93,629 in 2025. This is only an overall average and does not mean that every victim lost this amount.

There is also evidence of intervention through the Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS). By December 2025, more than ₹8,189 crore had reportedly been saved



across 23.61 lakh complaints. In this context, “saved” means money that was prevented from being syphoned off; it should not be taken to mean that the same amount was later recovered or refunded to victims.

Overall, the figures point towards a substantial increase in reported cybercrime and financial fraud, as well as the amount of money involved. However, these figures only reflect reported incidents. Changes in public awareness, reporting practices and categorisation may also affect the numbers. Further, the available data does not clearly show how each complaint moves from reporting and investigation to forensic examination, prosecution, trial and conviction.

4.7. Consistency, Gaps and Robustness of the Analysis

The material presented has certain limitations that should be taken into account when reading the findings. Cybercrime is sometimes underreported or recorded inconsistently. In addition, different agencies may utilise different categorisations, and there are few standardised indicators, making it difficult to assess the overall level of cybercrime. This is especially true for deepfake-related fraud, which is not specifically separated out in the data presented.

Cross-border cybercrime can also lead to practical challenges, as the perpetrator, victim, digital evidence, platform and/or proceeds of crime may be in different countries, which can make obtaining evidence or assistance from other countries’ authorities challenging.

Another challenge is the rapid evolution of technology and fraud schemes, including deepfake-related fraud, which may not always fit within existing legal categories or require different provisions to be interpreted depending on the context of each case.

These limitations do not render the material presented unusable; nevertheless, they should be taken into account when interpreting the results. In addition, the analysis indicates a disconnect between the formal availability of relevant legal provisions and the availability of information on their implementation in investigations, prosecutions, and trials.

4.8. Key Findings

The analysis shows that India already has different laws that can be used to deal with cybercrime and digital fraud. However, applying these laws to newer forms of fraud is not always simple. Deepfake-related fraud,



for example, is not covered by a separate offence, so existing provisions may have to be applied depending on the facts of each case. The case law further indicates that the principal challenge is not the complete absence of legal remedies but the application of general offences and evidentiary rules to AI-generated content whose source, authenticity, attribution and circulation may be difficult to establish.

Another important finding is that having a legal remedy does not always mean that the victim will recover the lost money. Quick reporting, proper investigation and coordination between authorities play an important role. Electronic evidence, identifying offenders and dealing with online intermediaries also remain difficult in many cases. The data reviewed shows a major rise in reported cybercrime and financial fraud. At the same time, the available figures do not clearly show what happens to complaints after reporting.

Overall, the findings show that the existing framework covers many forms of cybercrime, but practical and legal difficulties remain, especially with newer digital frauds.

4.9. Results

Based on existing studies and data analysis performed in our study, we present policy recommendations to modernise legal frameworks in India to keep up with evolving deepfake technology.

1) Section 319 of the BNS punishes 'cheating by personation'. In established Indian law interpretations, personation requires pretending to be a specific, identifiable natural or legal person (living or dead). In digital arrest and financial fraud scams, completely made-up or otherwise known composite personas are created who do not have a real-world equivalent. The defence counsel could argue such fictional personas do not meet the statutory 'personation', forcing prosecutors to resort to Section 318 (general cheating) or other sections imposing lighter penalties. The law needs to explicitly clarify that 'personation' also involves personas and digital representation of officials generated using synthetic media who do not exist in the physical world.

2) The process of digital restitution is complex, often taking years before victims get their money back. Releasing the funds requires an order of property disposal from a competent magistrate under sections 497 and 503 of BNSS, 2023. Because mule accounts often involve interstate jurisdictions and multi-layered bank hops, magistrates refuse to order pretrial release without hearing every account holder, who are usually



untraceable in such cases. When Section 503 is read with Section 107 BNSS (Attachment of proceeds of crime), a special procedural rule should be included stating that money electronically frozen using the 1930 helpline, when remains uncontested by the mule account holder for a period of 30 days following the statutory digital notice, will be issued an 'Interim Digital Restitution Order'. The intermediary financial institutions should be mandated to disburse the frozen sum back to the victim's account upon the victim signing an indemnity bond under Section 503(2) BNSS.

3) Section 79 of the IT Act grants intermediaries conditional safe-harbour immunity for third-party content, provided they act as passive hosts and adhere to due diligence mandates. Although the MeitY IT Amendment Rules (regarding SGI) mandate labelling and automated takedowns, they operate on a reactive notice-and-takedown model. A new proposal would be to implement mandatory upstream watermarking using cryptography and tamper-evident metadata at the generation layer. The GenAI infrastructure providers should be labelled as 'critical' entities. If they fail to watermark, they are bound to lose the safe-harbour immunity under Section 79. It creates a clear intermediary liability, increasing accountability.

5. CONCLUSION AND DISCUSSION

This study finds that the legal and institutional environment to combat cybercrime and digital fraud is overwhelmed by the increasing complexity and volume of fraud. The cybercrime reports registered in the National Cyber Crime Reporting Portal increased from 452,429 cases in 2021 to 2,268,346 in 2024. The aforementioned data demonstrates India's digital ecosystem is under serious strain; however, the statistics only record complaints and do not show whether deepfake or related crimes are widespread or what proportion of complaints are resolved from registration to investigation, prosecution, conviction, and restitution. Fraud is becoming exponentially more complex, and India does not have a specific statute that criminalises malicious deepfake or artificial intelligence impersonation, although existing laws partially cover some of these activities. Fraud detection is not the same as proving perpetrator responsibility; proving the involvement of an offender in a deepfake requires additional steps, including authenticating and preserving electronic evidence, which can be resource-intensive for investigators and prosecutors. The six dimensions identified in this study are interconnected and not isolated, meaning that a weakness in any of these areas affects the overall performance of the other areas. The relevant provisions, including the Information Technology Act 2000,



BNS 2023, BNSS 2023, BSA 2023, and 2026 IT Rules, cover various aspects of digital fraud, including cheating, personation, identity theft, forgery, and obscenity, but do not criminalise deepfake, leaving gaps in legislation, for which courts have to rely on certain general provisions that may not be entirely applicable to deepfake impersonation. At the same time, the combination of the aforementioned laws creates confusion in the interpretation, particularly in financial fraud crimes, where deepfake impersonation blurs the previously existing concepts, thereby creating a grey area in the understanding of financial fraud using synthetic media. Victim protection goes beyond preventing victimisation, including reporting, freezing funds, investigation, and actual recovery of money; these aspects are separate and must be considered independently. BNSS 2023 contains compensation provisions; however, until the mechanisms for their accessibility become fully operational, deepfake victims will not be able to rely on them. The critical aspect of institutional coordination is evident, as all the components of the enforcement chain fall under different jurisdictions, including banks, payment gateways, processors, investigators, prosecutors, and courts; each of these elements has limited clarity about its role in the context of deepfake fraud, which creates challenges at every stage. The cross-border nature of such crime adds another level of complexity, as does the inadequacy of international cooperation mechanisms, including

Mutual Legal Assistance Treaties and bilateral agreements, to the speed of digital evidence, platforms, and money transfer; even though formal mechanisms exist for evidence, platforms, and funds, their application can be too slow to respond to the realities of deepfake fraud. Addressing the identified gaps in institutional accountability and victim protection requires statutory amendments that explicitly define malicious deepfake impersonation as actionable personification to prevent legal technicalities from shielding offenders, as well as the introduction of an “Interim Digital Restitution Order” that would enable faster access to funds by victims of impersonation fraud. Finally, clarifying the liability of GenAI developers by obliging them to adopt watermarking at the input prompt level creates a legal precedent that will prompt the adoption of appropriate measures by developers to protect their safe harbour immunity by preventing fraudulent use of their technology, which would contribute to proactive liability. By examining deepfake-enabled fraud as a series of interconnected legal, evidentiary, institutional, and recovery challenges, this study develops a reform-focused framework that moves beyond simply pointing to the absence of a specific deepfake offence. Lastly, the limitations of this study include the fact that the provided statistics do not give a complete indication of the scale of the problem or the extent of the burden, if any, on the enforcement system with respect to deepfake



fraud. The data does not indicate whether the situation has improved or worsened in terms of deepfake-related fraud after the introduction of the SGI obligations for deepfake. Further research is needed to better understand the dynamics of complaints in the criminal justice system and identify gaps in legislation or institutional capabilities that require attention in the context of deepfake impersonation fraud.

References:

- Westerlund, M. (2019). The Emergence of Deepfake Technology: A Review. *Technology Innovation Management Review*, 9(11), 39–52. <https://timreview.ca/article/1282>
- Grobler, M. M., & von Solms, S. H. (2009). *A best practice approach to live forensic acquisition* [Doctoral dissertation, University of Johannesburg]. University of Johannesburg Research Space. https://www.researchgate.net/publication/30511762_Modelling_live_forensic_acquisition
- Subair, S., Yosif, D., Ahmed, A., & Thron, C. (2022). Cyber crime forensics. *International Journal of Emerging Multidisciplinaries: Computer Science & Artificial Intelligence*, 1(1), 41–49. <https://doi.org/10.54938/ijemdc sai.2022.01.1.37>
- ICT Cyber Desk. (2016). Cybercrime and cyber-terrorism, January–March 2016. In *Cyber-terrorism activities report No. 16: January–March 2016* (pp. 24–34). International Institute for Counter-Terrorism. <https://www.jstor.org/stable/resrep09466.6>
- Arctic Wolf. (2024, April 19). A brief history of cybercrime. Arctic Wolf Blog. <https://arcticwolf.com/resources/blog/decade-of-cybercrime/>
- Singh, S. (2024). *Digital arrest: The modern-day cyber scam*. NITI Aayog. <https://www.niti.gov.in/node/1642>
- Ministry of Home Affairs. (2026, July 21). *National cybercrime data* [Press release]. Press Information Bureau. <https://www.pib.gov.in/www.pib.gov.in/Pressreleaseshare.aspx?PRID=2287039>
- Borwell, B., Jansen, J., & Stol, W. (2022). *The psychological and financial impact of cybercrime victimisation: A novel application of the shattered assumptions theory*. ResearchGate. https://www.researchgate.net/publication/348407809_The_Psychological_and_Financial_Impact_of_Cybercrime_Victimization_A_Novel_Application_of_the_Shattered_Assumptions_Theory
- Zhang, Y., Xian, L., & Schaub, F. (2025). *Experiencing deceptive AI: A qualitative study of deepfake fraud victimization*. USENIX Symposium on Usable Privacy and Security (SOUPS) 2025. <https://share.google/MfpMcyzqGxrpo7FNk>



- Dadà, V., et al. (2025). *The human factor of cybercrime*. ResearchGate. https://www.researchgate.net/publication/351207454_The_Human_Factor_of_Cybercrime?utm_source=gemini&hl=en-IN
- Mehta, S., Patil, H., & Meghani, M. (2025). Deepfake technology & financial frauds: Awareness, risks and prevention strategies. *European Economic Letters*, 15(2), 2472–2477. doi.org <https://www.eelet.org.uk/index.php/journal/article/view/3095>
- Shamo, S. A. (2025). *The DeepFake and its impact on trading signals*. SSRN. <https://share.google/Zg43e2ETFS208iLQH>
- Paramasivan, K., Jaiswal, A., Fernando, A., & Sudarsanam, N. (2026). Victim-centric approach to financial cybercrime: Exploring vulnerabilities in the Indian digital landscape. *Humanities and Social Sciences Communications*, 13, Article 1411. doi.org <https://www.nature.com/articles/s41599-026-07906-5.pdf>
- Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. Polity Press. https://www.researchgate.net/profile/David-Wall-7/publication/378013252_Cybercrime_The_Transformation_of_Crime_in_the_Information_Age_2nd_edition/links/65c36f3179007454976a5420/Cybercrime-TheTransformation-of-Crime-in-the-Information-Age-2nd-edition.pdf
- Brenner, S. W. (2006). Cybercrime nation: National security, cyberspace, and the law. *International Journal of Law and Information Technology*, 14(3), 304–326. https://www.researchgate.net/publication/287743943_Cybercrime_and_the_law_Challenges_issues_and_outcomes
- Hunton, P. (2011). The legal and forensic challenges of digital evidence. *Computer Law & Security Review*, 27(6), 612–620. <https://www.sciencedirect.com/science/article/abs/pii/S0267364910001688?via%3Dihub>
- Button, M., Lewis, C., & Tapley, J. (2014). Not a victimless crime: The impact of fraud on individual victims. *Security Journal*, 27(1), 36–54. <https://psycnet.apa.org/record/2014-03316-003>
- Duggal, P. (2021). *Cyber law in India*. Wolters Kluwer. <https://www.scribd.com/document/1037962222/Textbook-on-Cyber-Law-Pavan-Duggal-2021-111226523-Libgen-li>
- In re: Victims of digital arrest related to forged documents, Suo Motu Writ Petition (Criminal) No. 3 of 2025 (Supreme Court of India, October 17, 2025).
- The State of West Bengal v. Jatin Anup Ladwal and Ors. Nadia District, West Bengal, India. (Kalyani Additional Sessions Court, Nadia District, West Bengal, July 17, 2025).



- Eswaramoorthi, R. (2026). Cross-border cybercrime jurisdiction and digital evidence admissibility: A comparative legal framework. *Sirashmi Perspectives in Cyber Law, Intellectual Property, and Legal Studies*, 1–19. <https://sirashmi.com/journals/index.php/SPCLIPLS/article/view/25>
- United Nations. (n.d.). United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes (Chapter XVIII, No. 18-16). United Nations Treaty Collection. https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-16&chapter=18&clang=en
- DD India. (2026, September 26). *EAM Jaishankar signs UN convention against cybercrime*. <https://ddindia.co.in/2026/09/eam-jaishankar-signs-un-convention-against-cybercrime/>
- X v. Union of India*, 2023 INSC 919 (Supreme Court of India, October 16, 2023).
- IJLLR Journal. (2026, June 21). *Deep Fakes And Indian Criminal Law: Challenges and Regulating Gaps In The Age Of AI*. IJLLR Journal. <https://www.ijllr.com/post/deep-fakes-and-indian-criminal-law-challenges-and-regulating-gaps-in-the-age-of-ai>
- Chaitanya Rohilla v. Union of India, W.P.(C) [PIL on AI Regulation] (High Court of Delhi 2023). <https://asiaiplaw.com/section/ip-analysts/pil-filed-in-delhi-high-court-addressing-unauthorized-use-of-artistic-works-by-ai>
- Parliament of India, Committee on Empowerment of Women. (2026, March 23). *Cyber crimes and cyber safety of women* (Report Summary). PRS Legislative Research. <https://prsindia.org/policy/report-summaries/cyber-crimes-and-cyber-security-of-women>
- X v. State (NCT of Delhi)*, W.P.(Crl) [Deepfake Takedown Order] (High Court of Delhi 2026).
- Calcutta High Court transfers the Rs 2.7 crore digital arrest scam case to CBI. (2026, September 23). *The Times of India*. <https://timesofindia.indiatimes.com/city/kolkata/calcutta-high-court-transfers-rs-2-7-crore-digital-arrest-scam-case-to-cbi/articleshow/134444246.cms>
- Ministry of Home Affairs. (2026a, February 4). *Indian Cyber Crime Coordination Centre (I4C)* [Press release]. Press Information Bureau, Government of India. <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2223095>



Ministry of Home Affairs. (2026b, February). *Indian Cyber Crime Coordination Centre (I4C) operational metrics* [Press release]. Press Information Bureau, Government of India. <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2226441>

Ministry of Home Affairs. (2026c, August 21). *Protecting citizens from digital fraud held in Kohima* [Press release]. Press Information Bureau, Government of India. <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2301973>

Anvar P. V. v. P. K. Basheer, (2014) 10 Supreme Court Cases 473 (Supreme Court of India).

Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 Supreme Court Cases 1 (Supreme Court of India)

Tomaso Bruno v. State of Uttar Pradesh, (2015) 7 Supreme Court Cases 178 (Supreme Court of India).

Shreya Singhal v. Union of India, (2015) 5 Supreme Court Cases 1 (Supreme Court of India)

State Bank of India v. Pallabh Bhowmick, 2025 INSC 102 (Supreme Court of India, January 3, 2025).

Miglani, S., & Parihar, R. (n.d.). Digital arrest scam in India: What does the law say? Neeti Niyaman. <https://neetiniyaman.com/digital-arrest-scam-in-india/>