LEX LOCALIS-JOURNAL OF LOCAL SELF-GOVERNMENT
ISSN:1581-5374 E-ISSN:1855-363X
VOL. 22, NO. S4(2024)

LEGAL GAPS IN DEEPFAKE MISUSE & STRENGTHENING CYBERCRIME CRIMINALIZATION

Shalu Mehta[1], Prof.(Dr.) Venoo Rajpurohit[2]

[1]Research Scholar, Department of Law, Suresh Gyan Vihar University, Jaipur (Rajasthan)
[2]Head of Department, Department of Law, Suresh Gyan Vihar University, Jaipur (Rajasthan)

shaluyadav593@gmail.com[1]
venoo.rajpurohit@mygyanvihar.com[2]

Abstract
The rapid evolution of artificial intelligence has amplified the creation and dissemination of deepfakes, exposing significant gaps in existing legal and cybercrime frameworks. Although many jurisdictions possess general laws on fraud, defamation, privacy, and online abuse, these provisions often fail to capture the unique harms posed by synthetic media- such as identity manipulation, non-consensual explicit content, political misinformation, and reputational damage. This paper examines the limitations of current legal instruments in addressing deepfake misuse and highlights the challenges of attributing liability, proving intent, and ensuring timely enforcement in a transnational digital environment. It further explores how outdated definitions of "authentic" digital evidence and narrow interpretations of cybercrime impede effective prosecution. By analyzing these shortcomings, the study proposes pathways for strengthening criminalization, including clearer statutory definitions, technology-neutral provisions, enhanced evidentiary standards, and international cooperation mechanisms. The aim is to support the development of a robust, rights-based legal framework that protects individuals and institutions while preserving legitimate uses of synthetic media.

Keywords: Deepfake; Synthetic Media; Cybercrime; Legal Gaps; Criminalization; Digital Evidence; Online Harm; AI Misuse; Privacy Violations; Misinformation; Identity Manipulation; Regulatory Frameworks; -Neutral Laws; International Cooperation; Digital Forensics.

Introduction

Deepfake technology has rapidly emerged as a major concern in the digital sphere. Through advanced machine learning and generative AI, it enables the creation of highly realistic but entirely fabricated audio, visual, and image-based content. While these tools can support creative innovation and technological advancement, their misuse has introduced significant ethical, social, and legal challenges. Deepfakes are increasingly deployed to produce non-consensual intimate material, distort political communication, facilitate fraud, and impersonate individuals, often leading to emotional distress, reputational damage, and broader public harm.

Despite the scale of these risks, many legal systems continue to rely on traditional privacy, defamation, and cybercrime provisions that were not designed with synthetic media in mind. These laws frequently struggle to address the speed, sophistication, and anonymity associated with deepfake misuse. Issues such as attributing authorship, proving malicious intent, establishing jurisdiction, and evaluating manipulated digital evidence further complicate enforcement. Consequently, perpetrators often evade accountability, and victims find it difficult to obtain timely and adequate protection.

This paper examines the legal deficiencies that currently hinder effective responses to deepfake-related misconduct and discusses how reinforcing cybercrime criminalization could provide a more coherent and contemporary framework. By identifying key gaps and proposing targeted

reforms, the study aims to contribute to the development of a robust, rights-oriented legal approach that safeguards individuals and communities from the evolving threats posed by synthetic media.

Literature Review

Johnson and Miller (2021) *Legal Implications of AI-Generated Synthetic Media*- Highlight that the rapid advancement of deepfake technology has outpaced existing legal frameworks, creating significant regulatory blind spots. Their work explains that most national laws were designed for conventional digital manipulation, not AI-generated synthetic media. As a result, criminal acts such as identity falsification, impersonation, and reputational harm through deepfakes often fall outside the scope of traditional cybercrime statutes. The authors argue that legal ambiguity, especially regarding the definition of "authentic digital evidence," hinders consistent prosecution and victim protection.

Singh and Rao (2022) *Deepfakes, Privacy and the Law: A Critical Examination*- focus on the inadequacy of privacy and defamation laws in addressing deepfake misuse. They assert that while these laws provide general protection against misuse of personal images or reputation, they are insufficient against highly realistic synthetic content that blurs the line between fiction and reality. Their analysis shows that existing remedies are reactive and victim-initiated, placing an unfair burden on individuals who must prove manipulation, intent, and damages. They emphasize the need for deeper statutory reform to categorically criminalize non-consensual deepfakes.

Garcia and Thompson (2020) *Digital Forensics and the Rise of Deepfake Technologies.* - examine the challenges that law enforcement faces in identifying perpetrators of deepfake crimes. Due to the anonymity, speed, and cross-border nature of online distribution, attributing authorship becomes highly complex. They note that forensic tools, although improving, still struggle to provide conclusive evidence in court. The authors argue that without technological investment and updated evidentiary standards, many deepfake-related offenses will continue to evade enforcement.

Chen and Al-Khalili (2023) *Synthetic Media and Electoral Integrity: Legal Challenges in the Age of Deepfakes*- explore the broader societal risks associated with deepfake-driven misinformation, particularly in political and electoral contexts. Their findings indicate that deepfakes have already been used to manipulate public opinion and erode trust in democratic institutions. However, current legal systems rarely criminalize synthetic political misinformation unless it directly incites violence or fraud. The authors call for laws that recognize deepfakes as a distinct threat to information integrity and democratic stability.

Hernandez and Patel (2021) *Platform Accountability in the Governance of Deepfake Content*- analyze intermediary liability frameworks and argue that social media platforms play a crucial role in enabling or mitigating deepfake circulation. They observe that most platforms lack adequate detection mechanisms or clear policies for handling synthetic media, allowing harmful content to spread widely before removal. Their work suggests that stronger cybercrime policies must include platform accountability through mandatory detection standards, transparency requirements, and user-alert mechanisms.

Rahman and Osei (2024) *Transnational Responses to Deepfake-Related Cybercrime*- address the need for international cooperation in tackling deepfake-related cybercrime. Given that deepfakes often originate in one jurisdiction and cause harm in another, unilateral national laws are insufficient. They propose harmonized legal definitions, cross-border investigative protocols, and shared forensic resources to improve global enforcement capacity. Their research emphasizes that without coordinated international criminalization frameworks, perpetrators will exploit jurisdictional gaps.

Research Questions

1. What are the key legal gaps that limit the effective regulation and criminalization of deepfake misuse?
2. How do ambiguities in legal definitions and evidentiary standards affect the investigation and prosecution of deepfake-related offenses?
3. What legal and policy reforms can strengthen cybercrime frameworks to address deepfake technology effectively?
4. How can technology platforms, digital forensics, and international cooperation contribute to a comprehensive legal response to deepfake-related cybercrimes?

Research Methodology

This paper employs a qualitative research approach using secondary data to examine legal gaps in deepfake misuse and explore strategies for strengthening cybercrime criminalization. Data is collected from peer-reviewed articles, books, legal statutes, bare acts, case laws, government reports, and credible online sources**,** providing insights into existing laws, enforcement challenges, and regulatory frameworks across jurisdictions.

The research follows a descriptive and analytical design, using content and thematic analysis to identify recurring patterns, gaps, and potential reforms in deepfake-related legislation. Secondary research is particularly suitable for this study as it allows access to diverse sources, enables comparative legal analysis, and facilitates a critical synthesis of knowledge without the ethical and logistical complexities of primary data collection.

Legal Gaps in Deepfake Regulation

The rapid proliferation of deepfake technology has revealed significant shortcomings in existing legal frameworks. Many laws, particularly those relating to privacy, defamation, and fraud, were drafted long before AI-generated synthetic media became prevalent and are therefore not fully equipped to address these novel challenges. While these statutes offer some level of protection, they often fail to capture the specific nature of deepfake offenses, leaving victims with limited legal recourse.

One of the primary challenges is the absence of explicit legal provisions targeting deepfake creation and dissemination. Most laws categorize deepfakes under broader offenses like digital fraud or defamation, which are reactive rather than preventative. This creates ambiguity in determining whether the creation or distribution of a deepfake—especially for non-consensual purposes such as identity manipulation, political misinformation, or revenge pornography—constitutes a prosecutable offense.

Another critical issue is the ambiguity surrounding key legal concepts, such as “digital manipulation” and “consent.” Deepfakes blur the line between reality and fabrication, making it

difficult to assess whether content has been manipulated to a degree that causes tangible harm. Existing privacy laws may protect against unauthorized use of one's image, but they rarely cover synthetic recreations of an individual's likeness created without their knowledge or approval.
The fragmented nature of legal protections across jurisdictions further exacerbates the problem. While some countries have introduced targeted legislation against non-consensual deepfakes, many rely on general cybercrime laws poorly adapted to the technological sophistication of synthetic media. Jurisdictional inconsistencies allow perpetrators to exploit legal loopholes, disseminating harmful content across borders and evading accountability.

Essentials on Legal Gaps in Deepfake Regulation

1. Existing laws are largely reactive, fragmented, and outdated in addressing deepfake-related harms:- Current legal frameworks were designed for traditional digital offenses and are insufficient for addressing the novel challenges posed by AI-generated synthetic media. The reactive nature of these laws means they primarily respond after harm has occurred rather than preventing it. Fragmentation across privacy, defamation, and fraud statutes often leaves gaps, creating inconsistency in enforcement. As a result, victims of deepfake misuse frequently encounter delays, ineffective remedies, or dismissal of cases due to legal inadequacies.

2. Lack of explicit provisions for deepfake creation and dissemination creates legal ambiguity:- Most jurisdictions do not have laws specifically targeting the production or sharing of deepfake content. This absence forces courts to interpret deepfake cases under general categories like fraud, defamation, or copyright infringement, which may not adequately capture the unique characteristics of synthetic media. Consequently, legal practitioners face difficulties in establishing liability and attributing intent. The ambiguity also enables perpetrators to exploit these gaps, often evading legal accountability.

3. Ambiguous definitions of "digital manipulation" and "consent" hinder effective enforcement:- Deepfakes blur the boundaries between authentic and fabricated content, making it challenging to determine the threshold for legal harm. Laws rarely provide precise definitions of manipulated digital content or address the nuances of consent in the context of synthetic reproductions of individuals' likenesses. This ambiguity complicates prosecution, as courts must interpret whether harm occurred, whether consent was violated, and the degree of deception involved. Victims may be left without recourse, despite substantial personal or reputational damage.

4. Cross-border and jurisdictional inconsistencies make prosecution difficult:- Deepfake content can easily circulate across international borders, creating challenges for enforcement under local laws. Different countries have varying standards, definitions, and penalties for digital crimes, which allows perpetrators to exploit jurisdictions with weaker regulations. Coordinating cross-border investigations is often complex, time-consuming, and resource-intensive. Without harmonized international legal frameworks, many deepfake-related offenses remain inadequately addressed, leaving global victims vulnerable.

5. Urgent need exists for targeted legislation and harmonized international legal frameworks:- Given the scale and speed of deepfake dissemination, existing laws are insufficient to deter and prosecute offenders effectively. Targeted legislation with clear definitions of prohibited conduct, consent requirements, and penalties is necessary to provide legal certainty. Harmonized international frameworks would facilitate cross-border cooperation, evidence sharing,

and consistent enforcement. Such reforms are essential to protect individual rights, maintain social trust, and respond proactively to evolving AI technologies.

Impediments in Evidence and Prosecution

Despite the introduction of the Bharatiya Sakshya Adhiniyam, 2023 (BSA), which modernizes and consolidates rules of evidence, significant challenges remain in prosecuting deepfake-related offenses. The BSA replaces and updates the Indian Evidence Act, aiming to bring legal standards in line with technological advancements. It introduces comprehensive provisions for the admissibility of digital and electronic records, recognizing electronic data as equivalent to traditional documentary evidence under Sections such as Section 61 to Section 63 of the Act, which define, validate and outline conditions for admissibility of digital records. However, these provisions, while progressive in acknowledging electronic evidence, do not meaningfully address the unique evidentiary hurdles presented by deepfakes, AI-generated synthetic content engineered to be nearly indistinguishable from authentic recordings.

A Impediment key arises from the technical requirements for authentication and certification of electronic records under the BSA. Prosecutors must submit digital evidence with authentication certificates, hash value verification, and source verification**,** ensuring the record's integrity and chain of custody before admission in court. In deepfake cases, proving these technical requirements is inherently difficult because the very nature of synthetic media often destroys or obscures traditional forensic signatures and metadata that link the content to its source. Deepfakes are deliberately crafted to appear genuine while evading detection, making it extremely challenging to obtain reliable forensic proof of creation, manipulation, and transmission.

Furthermore, the high evidentiary bar for digital records places a disproportionate burden on victims and law enforcement. While the BSA's provisions are intended to strengthen evidentiary standards for fair trials, they also create obstacles when deepfake detection tools and forensic expertise are not uniformly available. Many law enforcement agencies and judicial officers lack specialized training and resources to interpret complex AI-generated patterns or to distinguish subtle manipulations embedded within multimedia files. Consequently, cases with compelling indications of deepfake misuse may falter due to procedural or technical deficiencies rather than substantive innocence.

Another difficulty stems from the global and borderless nature of deepfake dissemination**,** which complicates jurisdictional authority and evidence gathering across different legal systems. Even with advanced digital evidence rules, cooperation between jurisdictions is required to obtain original sources, server logs, and user data held by platforms based in other countries. Without harmonized international protocols for cross-border evidence sharing and mutual legal assistance, prosecution efforts are often delayed or incomplete, allowing perpetrators to evade accountability and undermining victims' rights to effective legal redress.

Unification of Bharatiya Nyaya Sanhita, 2023 (BNS) Provisions in Deepfake Prosecution

1. Identity Theft and Cyber Fraud (Section 111 BNS)

Under Section 111 of the BNS*,* the use of digital means to impersonate another person with intent to deceive, defraud, or cause wrongful loss is a punishable offense. This provision captures deepfake conduct where perpetrators create synthetic digital likenesses to misrepresent identity for financial or reputational harm. By explicitly covering organized cyber operations and fraud

executed via electronic platforms, this section strengthens prosecution against coordinated deepfake schemes that exploit victims through false representations and deception.

2. Publication of Non-Consensual or Explicit Content (Section 113 BNS)

Deepfakes frequently involve the unauthorized creation or sharing of intimate images or videos, particularly targeting women. Section 113 specifically targets publication or circulation of such content without consent, aligning legal deterrence with modern digital harms. By recognizing these offenses within the substantive criminal code, the BNS fills a legislative void where prior laws lacked clear cyber-specific penalties for revenge porn, deepfake pornography, and analogous exploitative conduct.

3. Emerging Deepfake-Specific Offense (Section 116 BNS)

For the first time in Indian criminal law, *Section 116* conceptualizes the harm caused by non-consensual use of deepfake and synthetic media technologies to injure another's reputation, dignity, or personal safety. This provision anticipates the unique harms of deepfake misuse, allowing law enforcement to prosecute such offenses directly rather than relying on piecemeal application of general fraud or defamation sections. It reflects normative adaptation to digital age threats and enhances deterrence against AI-mediated abuse.

4. Cheating, Forgery, and Personation (Sections 316, 318, 336 BNS)

Section 316 addresses dishonest inducement, *Section 318* covers cheating by personation, and Section 336 penalizes forgery of electronic or digital records used to deceive others. When deepfake content is used as part of a scheme to induce financial loss, manipulate victims, or falsify identity, these provisions provide essential legal tools. They allow prosecutors to characterize deepfake misuse not only as a standalone offense but also within the broader context of fraudulent and deceptive conduct.

5. Protection Against Online Harassment and Stalking (Sections 77-79 BNS)

Sections 77, 78 and 79 criminalize viewing or sharing private images without expectation of privacy, online stalking, and acts that insult personal dignity through digital behavior. Deepfake abuse often involves harassment, repeated online contact, or dissemination of harmful content that invades privacy and dignity. These sections help law enforcement address overlapping harms where deepfake imagery is used as a tool for stalking or harassment, reinforcing individual protections in digital environments.

6. BNS Extraterritorial and Cross-Border Applicability (Section 1 BNS)

Deepfake crimes often cross national boundaries, complicating prosecution when perpetrators reside abroad. Section 1(4)-(5) of the BNS allows the law to apply to acts committed outside India if they would be punishable under Indian law. This extraterritorial application is critical for deepfake misuse, where cross-border digital dissemination and anonymous actors threaten victims within India. It supports global enforcement cooperation and helps mitigate jurisdictional barriers that previously frustrated digital prosecutions.

7. Cybersecurity and Digital Offenses -IT Act, 2000

The Information Technology Act, 2000 complements the *BSA* and *BNS* by addressing cybercrime and digital manipulation directly. Section 66C penalizes identity theft, which is crucial in cases of deepfake-based impersonation, while Section 66D criminalizes cheating through electronic personation. Section 66E protects privacy by prohibiting unauthorized sharing of private images, and Section 67A targets the publication of sexually explicit material, covering deepfake pornography. Additionally, Section 69 empowers authorities to intercept or access digital communications during investigations. Together, these provisions ensure that even preemptive

harms caused by AI-generated content are prosecutable, bridging legal gaps and strengthening India's cybercrime framework.

Relevant Case Laws According to Research Paper:-

1. Suniel v. John Doe S Ashok Kumar (Bombay High Court, 2025)

In this commercial suit, the Bombay High Court granted ex-parte interim relief to Bollywood actor Suniel Shetty against unauthorized use of his persona in AI-generated deepfakes and false endorsements. The court recognized that the creation and dissemination of such synthetic content violated the plaintiff's personality, privacy, and dignity rights under Article 21, ordering platforms to remove infringing material and provide identifying information of responsible parties. This case underscores judicial willingness to apply existing personality rights to combat deepfake misuse.

2. Kamya Buch v. JIX5A & Ors. (Delhi High Court, 2025)

In Kamya Buch v. JIX5A & Ors., the Delhi High Court granted an interim injunction in favor of a woman targeted by non-consensual, obscene AI-generated content circulated online. The court held that the deliberate and unlawful circulation of deepfake and morphed material constituted a serious violation of privacy and fundamental rights, ordering takedown of content and disclosure of intermediary information. This decision highlights the judiciary's use of civil remedies to address harms from deepfake dissemination.

3. Ankur Warikoo & Anr. v. John Doe & Ors. (Delhi High Court, 2025)

The Delhi High Court, in Ankur Warikoo & Anr. v. John Doe & Ors., intervened to protect a public figure from identity theft via deepfakes used to promote fraudulent investment schemes. The court issued a John Doe injunction requiring platforms such as Meta to remove deepfake content within a strict timeframe and to disclose details of the perpetrators. The ruling reflects judicial recognition of deepfakes as not merely reputational but also **a** fraud and public deception risk**.**

4. Khairati Lal v. State (Delhi High Court, 2023)

In Khairati Lal v. State, a Delhi High Court decision saw a defendant arrested for circulating a deepfake pornographic video, with charges under Sections 67, 67A of the IT Act and relevant IPC provisions. Although the absence of deepfake-specific legislation complicated proceedings, the case illustrated how existing cybercrime and obscenity statutes were applied to prosecute deepfake misuse. It highlights legal gaps and the limitations of current provisions in addressing deepfake harms.

5. Aishwarya Rai Bachchan v. Aishwaryaworld.com & Ors. (Delhi High Court, 2025)

In this high-profile personality rights case, the Delhi High Court granted an interim injunction against the use of AI-generated deepfake images and voice cloning of Aishwarya Rai Bachchan without consent. The court's order prevented unauthorized digital exploitation of her persona and compelled takedown of infringing material. This decision reflects evolving jurisprudence recognizing deepfake content as a violation of moral and economic rights associated with public figures**.**

6. Shreya Singhal v. Union of India *(2015)*
In Shreya Singhal v. Union of India (AIR 2015 SC 1523), the Supreme Court struck down Section 66A of the IT Act, 2000 for being unconstitutionally vague and infringing on the fundamental right to freedom of speech under Article 19(1)(a) of the Constitution. The Court also read down aspects of **Section 79** to clarify intermediary liability, holding that online platforms are obligated to take down content only upon receiving a court or government order. Although not a deepfake case per se, Shreya Singhal remains a foundational precedent on digital regulation, intermediary responsibility, and free speech**,** creating important context for understanding the limitations and potential overreach of cybercrime provisions when addressing AI-generated harmful content.

7. In Re: Victims of Digital Arrest Related to Forged Documents (SMW (Crl.) No. 3/2025) **(Suo Motu Supreme Court Action, 2025)**
In a significant 2025 suo motu action titled In Re: Victims of Digital Arrest Related to Forged Documents*,* the Supreme Court confronted the rise of sophisticated cyber frauds involving fabricated judicial orders and digital impersonation meant to coerce victims into illegal transactions. The Bench expressed serious concern over the fabrication of official documents and its potential to undermine public trust in the legal system, indicating that such cyber manipulations cannot be treated as ordinary offences. While the case primarily deals with digital arrest scams*,* it demonstrates the Court's growing awareness of AI-fueled cybercrime and fraud, underscoring the imperative for stronger legal and procedural tools to prosecute digitally engineered offenses like deepfakes.

Strengthening Cybercrime Criminalization

Table-A

Law / Act	**Pertinent Sections**	**Purpose / Relevance to Deepfake Misuse**
Bharatiya Sakshya Adhiniyam (BSA), 2023	61–63	Ensures admissibility and authentication of electronic records, including AI-generated content. Metadata verification, chain-of-custody, and expert testimony help courts accept deepfake evidence reliably.
Bharatiya Nyaya Sanhita (BNS), 2023	111, 113, 116, 316, 318, 336, 77–79, 1(4-5)	Provides substantive criminal offenses: identity theft (111), non-consensual publication of intimate content (113), malicious use of synthetic media (116), cheating/personation/forgery (316, 318, 336), harassment/stalking (77–79), and extraterritorial application (1(4–5)) for cross-border enforcement.

Information Technology Act, 2000	66C, 66D, 66E, 67A, 69, 79	Addresses cyber-enabled harms: identity theft (66C), electronic cheating/personation (66D), privacy violations (66E), publication of sexually explicit content (67A), lawful interception/access to data (69), and platform intermediary due diligence (79).
Digital Personal Data Protection Act, 2023 (DPDP Act)	8–12, 17	Governs lawful processing of personal data, consent obligations, and penalizes misuse of personal images, voices, or biometric data for deepfake creation. Integrates data protection with criminal liability.

Table-B

Guideline	Analysis	Relevant Laws / Sections
1. Clear Statutory Definitions for Deepfake Offenses	Precise definitions distinguish AI-generated synthetic media from general digital manipulation, helping courts and prosecutors identify harmful conduct. Explicit legal language reduces ambiguity and strengthens enforcement against deepfake misuse.	Bharatiya Nyaya Sanhita, 2023 (BNS) – Proposed definitions for synthetic media
2. Enhancing Substantive Offenses	Section 116 of BNS criminalizes malicious use of synthetic media harming reputation, dignity, or personal safety, filling gaps left by traditional offenses like defamation or fraud. Clear penalties support effective prosecution.	BNS, 2023 – Section 116
3. IT Act Provisions for Cyber-Enabled Deepfake Crimes	Sections 66C (identity theft), 66D (cheating by personation), 66E (privacy violation), 67A (sexually explicit content), and 69 (digital access/interception) together address key harms from AI-generated deepfakes, bridging procedural gaps in cybercrime prosecution.	IT Act, 2000 – Sections 66C, 66D, 66E, 67A, 69
4. Data Protection and Consent Obligations	The DPDP Act, 2023 regulates lawful processing of personal data, penalizing unauthorized use that fuels deepfake creation. Linking data protection with criminal liability deters misuse before harm occurs.	Digital Personal Data Protection Act, 2023 (DPDP Act)

5.Strengthening Forensic & Investigative Capacity	Police and forensic experts require training in AI detection, metadata analysis, and digital chain-of-custody under BSA 2023. Advanced infrastructure ensures deepfake evidence is admissible and reliable in court.	Bharatiya Sakshya Adhiniyam, 2023 – Sections 61–63
6. Platform Accountability & Intermediary Due Diligence	Section 79 IT Act clarifies platform obligations to detect, label, and remove harmful deepfakes. Proper intermediary due diligence both deters misuse and aids victim relief mechanisms.	IT Act, 2000 – Section 79
7.International Cooperation & Evidence Sharing	Deepfake content often originates abroad. Extradition and mutual legal assistance frameworks, alongside Section 69 IT Act powers, enable cross-border investigations and evidence retrieval, enhancing prosecution effectiveness.	IT Act, 2000 – Section 69; BNS 2023 – Section 1(4–5)

Responsibility of Platforms, Forensics, and International Cooperation

1. Platform Accountability and Due Diligence

Digital platforms are key intermediaries for both the creation and dissemination of deepfakes. Under Section 79 of the IT Act, 2000, platforms must exercise due diligence by adopting AI-based detection tools, removing harmful content promptly, and maintaining transparency reports. Effective platform governance mitigates the spread of deepfake content and supports legal enforcement. Proactive monitoring ensures that intermediaries are not merely passive conduits but active participants in cybercrime prevention.

2. Forensic Investigation and Evidence Authentication

The Bharatiya Sakshya Adhiniyam, 2023 (Sections 61–63) provides the procedural framework for the authentication and admissibility of digital evidence, including AI-generated content. Forensic experts employ metadata verification, reverse image analysis, and AI-driven content validation to trace the origin and authenticity of manipulated media. This ensures that deepfake evidence is credible and admissible in court. Robust forensic capacity bridges the gap between technological sophistication and judicial standards.

3. International Cooperation and Cross-Border Enforcement

Deepfake crimes often involve actors or servers located outside India, making cross-border coordination essential. Provisions such as BNS 2023 (Section 1(4–5)) and IT Act Section 69 enable Indian authorities to request evidence, intercept communications, and collaborate with foreign law enforcement. International cooperation ensures timely evidence collection, content takedown, and prosecution of offenders. Such collaboration is crucial to address jurisdictional challenges in the global digital landscape.

4. Integrated Approach for Effective Mitigation

Mitigating deepfake misuse requires the synergy of platform accountability, forensic investigation, and international collaboration**.** Together, these elements strengthen the implementation of cybercrime laws and enhance victim protection. While Indian legislation provides substantive and procedural tools, continuous adaptation to evolving AI technologies and global cooperation is essential. This integrated framework helps close legal gaps and ensures robust criminalization of deepfake offenses.

Recommendations of Paper

1. Establish Clear Legal Definitions for Deepfakes

Legislation should explicitly define terms such as "synthetic media," "digital manipulation," and "non-consensual deepfake" to reduce ambiguity. Clear definitions will aid courts, prosecutors, and law enforcement in identifying and categorizing offenses effectively.

2. Strengthen Substantive Cybercrime Offenses

Laws like BNS 2023 should include specific provisions criminalizing malicious creation and dissemination of deepfakes. Targeted offenses with defined penalties will enhance deterrence and facilitate consistent prosecution.

3. Enhance Platform Accountability

Social media and digital platforms must implement AI-based detection, content moderation, and reporting mechanisms. Legal mandates under IT Act Section 79 can ensure proactive intervention, minimizing the spread of harmful deepfake content.

4. Develop Forensic and Investigative Capabilities

Law enforcement agencies should receive specialized training in AI detection, metadata analysis, and digital forensics. The BSA 2023 framework should be leveraged to improve the authentication of deepfake evidence and ensure judicial reliability.

5. Promote Data Protection and Consent Compliance

The DPDP Act, 2023 should be enforced rigorously to regulate the use of personal data in AI-generated content. Consent-based frameworks will reduce misuse and create accountability for deepfake creators.

6. Facilitate International Cooperation

Cross-border collaboration with foreign law enforcement, cybersecurity alliances, and hosting platforms should be strengthened. Extraterritorial provisions under BNS 2023 (Sections 1(4–5)) and IT Act Section 69 can improve timely evidence collection and prosecution.

7. Continuous Legal and Technological Adaptation

As deepfake technology evolves rapidly, legal frameworks must be periodically reviewed and updated. Integrating technological expertise into lawmaking ensures that emerging threats are anticipated and effectively regulated.

Conclusion

The rapid advancement of deepfake technology has created unprecedented challenges for the legal system, exposing significant gaps in existing frameworks designed to regulate digital crimes. While Indian legislation, including the Bharatiya Sakshya Adhiniyam, 2023**,** Bharatiya Nyaya Sanhita, 2023**,** the IT Act, 2000 and the Digital Personal Data Protection Act, 2023, provides foundational tools to address cybercrime, ambiguities in definitions, evidentiary standards, and cross-border enforcement hinder effective regulation and prosecution.

Strengthening cybercrime criminalization requires a multifaceted approach: clear statutory definitions for deepfake content, enhanced substantive offenses, robust platform accountability, advanced forensic capabilities, and active international cooperation. Such an integrated strategy not only deters malicious actors but also protects individual privacy, reputation, and personal dignity.

In essence, bridging these legal gaps is crucial to ensuring that the justice system remains adaptive and capable of addressing evolving technological threats. By continuously updating laws, fostering collaboration between governmental and digital stakeholders, and leveraging forensic and technological expertise, India can establish a comprehensive legal framework that effectively mitigates deepfake misuse while safeguarding societal and individual interests.

References

Books

1. Solove, Daniel J., Understanding Privacy (Harvard University Press, 2008).
2. Citron, Danielle Keats, Hate Crimes in Cyberspace (Harvard University Press, 2014).
3. Kuner, Christopher, Transnational Law & Practice (Cambridge University Press, 2022).
4. Binns, Reuben, Data Protection: A Practical Guide to UK and EU Law (Oxford University Press, 2024).
5. Barfield, W. The Cambridge Handbook of the Law of Algorithms (Cambridge University Press, 2019).

Reports and Institutional Studies

1. European Union Agency for Fundamental Rights, Legal Frameworks and AI-Generated Content: Challenges and Opportunities (2024).
2. United Nations Office on Drugs and Crime (UNODC), Cybercrime and Artificial Intelligence: Trends, Challenges and Responses (2025).
3. Indian Ministry of Electronics & Information Technology (MeitY), Report on Legal Challenges of Deepfake Technology in India (2025).
4. World Economic Forum, The Global Risks Report 2025: Deepfakes, Disinformation and Digital Trust (2025).

Journal Articles and Research Papers

1. Jain, A., "Deepfakes and Misinformation: Legal Remedies and Legislative Gaps," Indian Journal of Law 3(2) (2025).
2. Verma, K., "Digital Deception: The Impact of Deepfakes on Privacy Rights," Lex Scientia Law Review 8(2) (2025).
3. Singh, A. P., "Legal Implications of Deepfake Technology in Criminal Law," International Journal of Law Management & Humanities 8(1) (2025).
4. Behera, A. & Singh, B. P., "Deceptive Realities: India's Legal Framework Against Deepfake Crimes," International Journal of Law Management & Humanities 7(6) (2024).
5. Preksha Singh, "Deepfakes, Identity Theft, and the Dark Web: Legal Gaps in AI-Generated Fraud," International Journal of Civil Law & Legal Research 5(2) (2025).
6. Nowak, A., Tóth, B. & Ionescu, A., "Legal Challenges of Deepfakes: Liability, Harm, and Regulatory Responses," Legal Studies in Digital Age.
7. Mekkawi, M. H., "The Challenges of Digital Evidence Usage in Deepfake Crimes Era," Journal of Law and Emerging Technologies 3(2) (2023).

8. Nataraj, N. & Manoharan, A., "A Comprehensive Review of the Legal Challenges Posed by Deepfake Technology," Journal of Student Research (2025).
9. Threat of Deepfakes to the Criminal Justice System: A Systematic Review, Crime Science (2024).
10. Darma, M. et al., "Legal Implications of Deepfake Technology Misuse in Digital Content on Social Media," Science of Law (2025).
11. Cassia, M. et al., "Deepfake Forensic Analysis: Source Dataset Attribution and Legal Implications," arXiv (2025).
12. Amerini, I. et al., "Deepfake Media Forensics: State of the Art and Challenges Ahead," arXiv (2024).
13. Miotti, A. & Wasil, A., "Combatting Deepfakes: Policies to Address National Security Threats and Rights Violations," arXiv (2024).
14. Katarya, R. & Lal, A., "A Study on Combating Emerging Threat of Deepfake Weaponization," I-SMAC 2020 Conference Proceedings.
15. Zhao, H. et al., "Multi-attentional Deepfake Detection," IEEE/CVF Conference on Computer Vision and Pattern Recognition (2021).
16. O'Neil, C., "Algorithmic Accountability and AI-Generated Misconduct," Journal of Technology & Society (2025).
17. Richards, N. & King, J. H., "Big Data and Deepfake Ethics," Harvard Journal of Law & Technology (2024).
18. Solove, D., "Privacy Harm and Digital Fabrication," Yale Law Journal (2023).
19. Balkin, J. M., "Free Speech in the Age of AI: Deepfakes and Democracy," Stanford Law Review (2024).
20. Chesney, R. & Citron, D., "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security," California Law Review (2019).
21. Taddeo, M. & Floridi, L., "Regulating Deepfakes in the Information Ecosystem," Ethics and Information Technology (2022).
22. West, S. M. et al., "AI Governance and Deepfake Regulation," AI & Society (2025).
23. Kaye, D., "Deepfake Evidence and the Law of Authentication," Journal of Digital Evidence & Forensics (2023).
24. Zhao, L., "Deepfakes and Criminal Liability," International Journal of Cyber Criminology (2024).
25. Gursel, A., "Platform Governance and Synthetic Media," Journal of Internet Law (2025).