# DEEPFAKE CRIMES AND THE INDIAN CRIMINAL JUSTICE SYSTEM: LEGAL CHALLENGES, EVIDENTIARY ISSUES AND THE NEED FOR REFORM

*By Dr. Gaurav Kumar*[*] *& Tanisha Verma*[**]

**ABSTRACT**

*The research investigates how deepfake technology has led to increased criminal activities in India while assessing the Indian judicial system's response to new criminal laws. The research examines how deepfakes enable impersonation-based fraud and cause damage to people's reputation and leverage digital platforms to create public disturbances. The research maps common deepfake fact-patterns to relevant provisions of the Bharatiya Nyaya Sanhita, 2023, and evaluates procedural readiness under the Bharatiya Nagarik Suraksha Sanhita, 2023, particularly the handling of electronic complaints and documented seizure of digital devices. The assessment investigates the requirements for evidence presentation under the Bharatiya Sakshya Adhiniyam, 2023, which includes the processes for verifying and approving electronic document evidence. The study defines institutional limitations which affect police operations and cyber forensic investigations and legal processes and judicial evaluation of synthetic media content and presents suggestions for improving investigation methods and forensic capabilities and platform responsibility to achieve better victim protection and crime deterrence.*

**Keywords**: Deepfake crimes; Bharatiya Nyaya Sanhita, 2023; Bharatiya Nagarik Suraksha Sanhita, 2023; Bharatiya Sakshya Adhiniyam, 2023; Electronic evidence; Digital forensics.

[*] Assistant Professor, School of Law, IILM University, Greater Noida, India. Email – gaurav.kumar@iilm.edu.
[**] LLM Student, School of Law, IILM University, Greater Noida, India. Email - tanisha.verma.gnllm2026@iilm.edu.

## I. Introduction

Deepfake crimes refer to criminal misuse of synthetic media which uses machine-learning methods to create authentic-looking videos that enable criminals to perform acts of deception and humiliation and extortion and impersonation and incitement to violence.[1] The legal system in India now applies its new criminal law framework to handle deepfake cases which combine identity theft with reputational harm and threats and digital evidence from electronic records. The legal framework handles deepfake cases through the Bharatiya Nyaya Sanhita 2023 BNS and Bharatiya Nagarik Suraksha Sanhita 2023 BNSS and Bharatiya Sakshya Adhiniyam 2023 BSA which establish rules for evidence. Deepfake impersonation leads to fraud which BNS section 319[2] defines as cheating by personation while BNS section 356[3] handles reputational attacks as defamation and BNS section 351 defines coercive dissemination as criminal intimidation and BNS section 353[4] describes the manipulative circulation of false information "through electronic means" as a public-order violation. The deepfake functions as a falsified electronic record which makes BNS section 336[5] (forgery, including electronic record) and related rules about forged electronic records applicable.

Deepfakes create special threats to criminal justice systems because they convert realistic elements into lethal weapons which can be used for large-scale destructive purposes through synthetic clips. The most common victim-facing harms include sexualised deepfakes stalking-like monitoring reputational destruction blackmail and targeted harassment. The BNS categorizes through its section 77 which handles voyeurism all violations that involve non-consensual capture or sharing of intimate private act images. The second section digital surveillance activities which track people through their online activities together with their email and electronic communication will violate BNS section 78[6]. The section 351 of BNS criminalizes all types of threats that use coercion to accomplish compliance through

[1] Editor, "Emerging Technologies and Law: Legal Status of Tackling Crimes Relating to Deepfakes in India" *SCC Times*, 2023 *available at*: https://www.scconline.com/blog/post/2023/03/17/emerging-technologies-and-law-legal-status-of-tackling-crimes-relating-to-deepfakes-in-india/ (last visited May 10, 2026).
[2] LIVELAW NEWS NETWORK, "Magistrate Not Empowered To Take Recognisance Of Offence U/S 358 BNSS: Delhi High Court" *Live Law*, 15 September 2025.
[3] Divyansha Goswami, "Re-Imagining Kafka's Courtroom: Unpacking The Procedural Challenges Of Trial-In-Absentia Under The New..." *Live Law*, 8 October 2024.
[4] Live Law, "Read all Latest Updates on and about Section 353 Bharatiya Nyaya Sanhita" *Live Law available at*: https://www.livelaw.in/tags/section-353-bharatiya-nyaya-sanhita (last visited May 10, 2026).
[5] Justice V Ramkumar, "The Bharatiya Nagarik Suraksha Sanhita, 2023 ('BNSS' For Short) At A Glance-Comments By Justice ..." *Live Law*, 16 March 2024.
[6] Editor, "Clicking a woman not stalking under BNS: HP HC" *SCC Times*, 2025 *available at*: https://www.scconline.com/blog/post/2025/08/20/clicking-a-woman-not-stalking-under-bns-hp-hc/ (last visited May 10, 2026).

intimidation methods which include attacking a person's reputation.[7] The BNS section 353 framework enables us to evaluate the social damage which deepfake technology creates when it spreads fake news to generate public panic and hatred. The outcome of deepfake cases depends on the methods used to gather and maintain and verify and show electronic evidence during the court process.[8]

The BNSS system incorporates digital procedures into its investigation process through its section 173 which permits organizations to share information about cognizable crimes through electronic platforms. The BSA establishes a new electronic evidentiary process which enables proof of electronic record content through BSA section 62 while BSA section 63(4) defines conditions for admissibility and certificate requirements. BSA sections 85 and 86 create legal assumptions that courts can use to evaluate electronic agreements and secure electronic records which affects how authenticity and integrity arguments will be presented during digital trials.[9]

### *A. Meaning, Nature and Forms of Deepfake Technology*

Deepfake technology operates through algorithms which create or modify audio-visual content to produce convincing yet false fake representations that include face-swaps and lip-syncing and synthetic voice cloning and fully generated virtual identities. The legal system considers the output as an electronic document which people dispute because they question its authenticity. The deepfake becomes illegal when someone creates or modifies it to deceive others or to cause harm because its creation requires a target and BNS section 336 applies to document forgery with electronic record fraud. The BNS section 319 law defines cheating through impersonation as a crime which occurs when the perpetrator pretends to be another person for their own advantage or to inflict damage on others. Deepfake clips become admissible in court based on BSA sections 62 and 63 but section 63(4) requires a certification which contains technical details that prove the computer output.[10]

[7] Live Law, "Read all Latest Updates on and about Section 351 BNSS" *Live Law available at*: https://www.livelaw.in/tags/section-351-bnss (last visited May 10, 2026).
[8] Editor, "Emerging Technologies and Law: Legal Status of Tackling Crimes Relating to Deepfakes in India" *SCC Times*, 2023 *available at*: https://www.scconline.com/blog/post/2023/03/17/emerging-technologies-and-law-legal-status-of-tackling-crimes-relating-to-deepfakes-in-india/ (last visited May 10, 2026).
[9] Editor, "Section 173(3) BNSS Explained: FIR, Preliminary Enquiry & Legislative Intent" *SCC Times*, 2026 *available at*: https://www.scconline.com/blog/post/2026/01/17/section-173-3-bnss-statutory-interpretation-fir-registration/ (last visited May 10, 2026).
[10] Gagan Verma & Mahima Wahi, "Deepfakes, Due Diligence And The Good Samaritan Paradox; How India's 2026 IT Amendment Rules Resolve..." *Live Law*, 15 April 2026.

### *B. Growth of Deepfake Misuse in the Digital Environment*

The easy-to-use generative tools and anonymous distribution channels and platform virality have created a situation where deepfake technology gets used for impersonation scams and sexually explicit synthetic content and coordinated disinformation. Indian enforcement agencies establish their connections through identity deception and coercion methods because section 319 (cheating by personation) and section 336 (forged electronic records) and section 351 (person property or reputation threats) together define the details of impersonation-based scams.[11] Section 353 handles electronic distribution of false or frightening information which causes public harm through electronic means because it addresses public safety threats. Special cyber-law provisions exist to handle identity theft and online impersonation cases which use IT Act sections 66C and 66D together with IT Act sections 67 and 67A to control obscene and sexually explicit online content. Deepfake harms extend beyond general penal law because they involve both standard criminal offenses and technology-specific violations. [12]

### *C. Relevance of Deepfake Crimes to the Indian Criminal Justice System*

The criminal justice system faces its toughest test because deepfake crimes violate fundamental beliefs that people can trust their own vision while requiring law enforcement to act. BNSS provides important procedural hooks: section 173 recognises electronic reporting of cognizable offences; section 105 requires audio-video recording of search and seizure; and investigation design increasingly depends on forensic processes (including videography of evidence collection for serious offences), which is crucial when authenticity and chain-of-custody are contested. The BSA's electronic evidence system supplies trial standards through its main rules in sections 62 and 63 which include section 63(4) as a certification method.[13] The BNS law defines the common deepfake-related offenses as section 77 which penalizes unauthorized recording and distribution of private activities and section 78 which penalizes electronic monitoring-related stalking and section 351 which penalizes criminal threats and section 356 which penalizes defamation through spoken words or visual symbols. Deepfakes create

[11] NV Geetha, "The Anatomy Of A Cyber Fraud: How A Retired Police Officer Fell Prey To A Sophisticated Investment Scam" *Live Law*, 28 December 2025.

[12] Editor, "Chasing Deepfakes Across Borders & Protecting Rights" *SCC Times*, 2025 *available at*: https://www.scconline.com/blog/post/2025/11/08/deepfake-regulation-rights/ (last visited May 10, 2026).

[13] Bhumika Indulia, "Electronic Evidence in Focus: Navigating Legal Shifts in the Law on Electronic Evidence under the BSA, 2023" *SCC Times*, 2024 *available at*: https://www.scconline.com/blog/post/2024/10/23/electronic-evidence-in-focus-navigating-legal-shifts-in-the-law-on-electronic-evidence-under-the-bsa-2023/ (last visited May 10, 2026).

multiple problems which need to be solved through four different stages that include filing a complaint and conducting an investigation and gathering digital evidence and making court judgments.[14]

### *D. Objectives of the Study*

1. To investigate how BNS 2023 handles deepfake-driven behaviour which includes impersonation, intimidation, privacy violations, defamation, and creation of fake electronic documents.
2. To discover the specific obstacles which prevent people from filing complaints and conducting search and seizure operations and deepfake incident investigations according to the BNSS 2023 regulations.
3. To investigate how deepfake evidence can be admitted and acknowledged as trustworthy according to the BSA 2023 rules which include requirements for electronic records certification and integrity maintenance.
4. To examine how police forces and cyber units and forensic laboratories face obstacles while they work to detect and identify deepfake technology.
5. To recommend specific changes which will improve investigation standards and evidentiary practices and protective measures for deepfake victims in India.

### *E. Research Questions*

1. Which BNS 2023 provisions from core BNS services identify which deepfake threats according to their specific method of operation which includes impersonation and coercion and privacy invasion and reputational damage?
2. What impact does the BNSS, 2023, standards guide on electronic complaints as well as searches/seizures affect the quality of deepfake case investigations?
3. What is the main evidential hurdles vis-a-vis admitting and relying upon deepfake audio-visual material-electronic evidence under BSA, 2023?
4. How do chain of custody, forensic capacity, and attribution mitigation influence prosecution outcomes in the context of deepfake crimes?
5. What kind of legal and procedural reforms are necessary to ensure maximum deterrence while protecting freedom of speech and due-process rights?

[14] Aayushman Gaikwad & Smruti Mishra, "Three Hours To Comply: India's New Rules For AI-Generated Content And Deepfakes" *Live Law*, 21 February 2026.

### *F. Research Methodology*

The study uses doctrinal research methods to analyze primary legal materials through organized legal research. The study investigates BNS 2023 statutory provisions which address impersonation and intimidation and privacy invasion and defamation and electronic record falsification. The study investigates procedural requirements of BNSS 2023 which describe how to record electronic complaints and conduct investigations and execute search and seizure operations. The study examines BSA 2023 evidentiary rules which define how electronic records must be verified and accepted as evidence and treated under legal presumption. The research uses secondary sources which include policy documents and official government materials to establish enforcement difficulties and to create reform-oriented solutions that match chapter themes.

### *G. Review of literature*

**Jyothsna Gurumurthy (2024)**[15] existing Indian legal system fails to adequately address deepfake damages which require protection through a statutory system that needs to be created with better victim support and technical knowledge. The study provides essential information which enables researchers to study how India develops its regulatory system.

**Shimona Mohan and Sarthak Wadhwa, (2023)**[16] research investigates deepfake technology's impact on political communication and misinformation dissemination and democratic integrity, while demonstrating that insufficient regulations fail to control fabricated content which spreads through digital platforms.

**Maria-Paz Sandoval, Maria de Almeida Vau, John Solaas and Luano Rodrigues (2024)**[17] Through its systematic review, this study demonstrates how deepfake technology endangers criminal justice systems by eroding public confidence in digital proof and generating research doubts, which result in police departments and prosecutors and forensic analysts and court systems facing higher difficulties.

[15] Jyothsna Gurumurthy, "In the Pursuance of a Robust Legal Framework to Address Deepfake Harms: An Analysis of the Indian Legal Discourse," 20 *Indian Journal of Law and Technology* 1 (2024)
[16] Shimona Mohan and Sarthak Wadhwa, "Deepfakes and Shallow Laws: Regulating Distorted Narratives in the Political Cyberspace," 19 *Indian Journal of Law and Technology* 94 (2023)
[17] Maria-Paz Sandoval, Maria de Almeida Vau, John Solaas and Luano Rodrigues, "Threat of Deepfakes to the Criminal Justice System: A Systematic Review," 13 *Crime Science* 41 (2024)

**Felipe Romero-Moreno (2024)**[18] research examines deepfake technology through a human rights framework, which requires evaluation of its content according to free speech rights and personal dignity rights and privacy rights and the need for regulatory measures.

**Tyrone Kirchengast, (2020)**[19] research evaluates the need to establish specific criminal laws against deepfake production and distribution, while it examines the legal and policy challenges which control both deterrence and enforcement and offense proportionality for image-manipulation crimes.

**Alex Barber (2023)**[20] The article studies how deepfake regulations create a philosophical and legal conflict between freedom of expression and official restrictions that control false yet expressive content which includes parody and political speech and misinformation and deception.

**Bao Kham Chau and George, He (2025)**[21] article studies audio deepfakes to determine appropriate regulations for digital platforms and content hosts and creative intermediaries who use synthetic voice cloning to create deceptive and exploitative and misleading content.

**Noelle Martin (2025)**[22] article studies Australian eSafety regulations for online safety through their implementation which includes administrative enforcement and victim-centred takedown systems and institutional accountability to combat deepfake misuse.

**Parkhi Saxena and Gaurav Pathak (2025)**[23]article assesses deepfake technology through a feminist legal lens which shows how platform control and gender-based violence and privacy breaches and social inequality amplify the human rights violations caused by synthetic media.



[18] Felipe Romero-Moreno, "Generative AI and Deepfakes: A Human Rights Approach to Tackling Harmful Content," 38 *International Review of Law, Computers & Technology* 297 (2024)
[19] Tyrone Kirchengast, "Deepfakes and Image Manipulation: Criminalisation and Control," 29 *Information & Communications Technology Law* 308 (2020)
[20] Alex Barber, "Freedom of Expression Meets Deepfakes," 202 *Synthese* art. 40 (2023)
[21] Bao Kham Chau and George He, "Audio Deepfakes and the Regulation of the Landlords of Creativity," 1 *Cambridge Forum on AI: Law and Governance* e30 (2025)
[22] Noelle Martin, "Online Safety Regulation of Deepfake Abuse: A Case Study on Australia's eSafety Commissioner," 34 *Griffith Law Review* 23 (2025)
[23] Parkhi Saxena and Gaurav Pathak, "Deepfakes, Big Tech, and Human Rights Challenges: Examining the Technology from a Feminist Legal Lens," 29 *The International Journal of Human Rights* 1 (2025)

**Priyansh Nema (2021)**[24] article addresses deepfake technology for India by examining its misuse and legal ambiguities and the urgent requirement for improved local regulations which makes it particularly useful for Indian legal scholars who study doctrinal research.

### *H. Research gap*

The existing research about deepfakes studies five main topics which include privacy issues and misinformation problems and platform regulation and gender-based violence and the right to free speech. The current research about deepfake crimes under the new Indian criminal laws, which include the Bharatiya Nyaya Sanhita 2023 and Bharatiya Nagarik Suraksha Sanhita 2023 and Bharatiya Sakshya Adhiniyam 2023, remains incomplete. Most studies do not comprehensively examine the interaction between substantive offences, evidentiary rules, forensic attribution, and procedural investigation under the reformed criminal justice system. The Indian academic community has not yet developed sufficient research about the authentication process and prosecutorial methods and judicial evaluation of deepfake evidence in criminal cases.[25]

## II. DEEPFAKE CRIMES AND THEIR CRIMINAL DIMENSIONS IN INDIA

Deepfake crimes in India function as "compound" offenses because criminals use synthetic audio-visual content to carry out multiple criminal activities which include deceiving people and harming their reputation and breaching their privacy and doing public mischief and using coercive methods. The Bharatiya Nyaya Sanhita 2023 BNS serves as the primary legal framework which connects criminal behavior to different offenses which include cheating by personation BNS s 319 and forgery and forged electronic record use BNS ss 336 and 340 and criminal intimidation BNS s 351 and defamation BNS s 356 and statements which lead to public mischief through electronic means BNS s 353. The Bharatiya Nagarik Suraksha Sanhita 2023 BNSS and Bharatiya Sakshya Adhiniyam 2023 BSA together with their electronic evidence handling rules define the investigation and proof process for the case.[26]

[24] Priyansh Nema, "Deepfakes in India," 29 *International Journal of Law and Information Technology* 1 (2021)
[25] Editor, "Chasing Deepfakes Across Borders & Protecting Rights" *SCC Times*, 2025 *available at*: https://www.scconline.com/blog/post/2025/11/08/deepfake-regulation-rights/ (last visited May 10, 2026).
[26] Editor, "Emerging Technologies and Law: Legal Status of Tackling Crimes Relating to Deepfakes in India" *SCC Times*, 2023 *available at*: https://www.scconline.com/blog/post/2023/03/17/emerging-technologies-and-law-legal-status-of-tackling-crimes-relating-to-deepfakes-in-india/ (last visited May 10, 2026).

### *A. Deepfakes as Instruments of Fraud, Defamation and Identity Misuse*

Deepfakes enable fraud by simulating a trusted identity through three methods which include voice-cloned CEO calls and synthetic video instructions and face-swapped KYC clips. The legal elements of the offense which pursue impersonation and inducement demonstrate their connection to the actual operate of the system. The accused demonstrates BNS s319 cheating by personation through his act of pretending to be another person. BNS s336 and BNS s340 establish that a deepfake functions as a falsified electronic record which people use to deceive others. The Information Technology Act 2000 provides a dedicated cyber-offense track which includes the specialized tracks. This law enforcement approach proves effective when criminals conduct their illegal activities through web platforms and that detrimental behavior occurs through digital access points and their connected systems.[27]

The use of deepfake technology for defamation establishes a new form of damage because it combines fake evidence which appears real with its ability to spread online. The new penal code establishes BNS s.356 (defamation) as applicable when someone uses words or signs or visible representation through which deepfake video and manipulated audio become visible to others. The BNS definition of criminal intimidation expands to cover situations where people face reputational damage through threats which include "pay or the clip goes public" because BNS s.351 (criminal intimidation) defines threats as actions which damage a person's "reputation" while deepfake blackmail campaigns use hidden origin threats to blackmail their victims.[28]



### *B. Deepfakes and Offences Against Women, Children and Personal Dignity*

The use of deepfake technology in India threatens people through gender-based violence because it enables non-consensual creation of sexual deepfakes which lead to humiliation and harassment of victims and their personal dignity and bodily autonomy get violated by synthetic visual content. The BNS defines this specific offense through BNS s.77 (voyeurism) which makes it illegal to record and share private videos of women without their consent and BNS s.78 (stalking) which prohibits people from tracking a woman who uses internet and email and other electronic communication channels. Offenders use deepfake production to create harmful

[27] Aayushman Gaikwad & Smruti Mishra, "Three Hours To Comply: India's New Rules For AI-Generated Content And Deepfakes" *Live Law*, 21 February 2026.
[28] Editor, "Chasing Deepfakes Across Borders & Protecting Rights" *SCC Times*, 2025 *available at*: https://www.scconline.com/blog/post/2025/11/08/deepfake-regulation-rights/ (last visited May 10, 2026).

content because they take photographs from real people while they stalk their victims who reside on various online platforms so the authorities need to understand how s.78 (patterned pursuit/monitoring) together with s.351 (criminal intimidation) functions because criminals use these tactics to make victims stay silent or do what they want.[29]

The Information Technology Act of 2000 provides additional legal framework for BNS because it criminalizes the electronic distribution of obscene and sexually explicit content through IT Act sections 67 and 67A. Deepfake pornography and synthetic intimate clips, even when "generated" rather than recorded, often fall within this electronic-publication architecture, which provides investigators with extra legal options to pursue charges that match the way content is shared online. The overlap matters in practice because deepfake abuse typically involves platform-hosting and re-uploading and international content distribution while IT Act violations permit authorities to obtain devices and extract data which helps them trace the content production process and identify the individuals who uploaded it. [30]

### *C. Public Disorder, Electoral Manipulation and Threats to National Security*

Deepfakes create public disorder because their design aims to generate panic which results in communal violence and they spread "false information" that seems real. The BNS addresses this risk through BNS s.353 (statements conducing to public mischief), which explicitly covers making, publishing, or circulating false information or reports "including through electronic means" with intent or likelihood of causing fear/alarm, inducing offences against the State or public tranquillity, or inciting offences between groups. [31]



The BNS introduces section 152 which defines act endangering sovereignty and unity and territorial integrity of India because it includes all forms of excitation and armed rebellion and subversive activities and all electronic communication methods that enable these activities to protect deepfake campaigns which separatist activities and hostile influence operations. The electoral domain faces integrity challenges through deepfakes because synthetic political ads and fake leader statements enable voter deception which creates fast track to extreme political division. The Election Commission of India has issued advisories addressing labelling of

[29] Sanhita Chauriha, "Are Deep Fakes Digital Chameleons?" *Live Law*, 30 September 2023.
[30] Bhumika Indulia, "Privacy Venture: The Extent of Data Retention" *SCC Times*, 2021 *available at*: https://www.scconline.com/blog/post/2021/02/15/data/ (last visited May 10, 2026).
[31] Editor, "Section 353 (2) BNS Archives" *SCC Times available at*: https://www.scconline.com/blog/post/tag/section-353-2-bns/ (last visited May 10, 2026).

synthetic/AI-generated content in political communication, which creates institutional pressure for transparency standards that will exist despite challenges of real-time criminal prosecution. This interacts with ongoing executive policy pathways under the IT governance framework that increasingly expects intermediaries to detect, label, and respond to synthetic media misuse as part of due diligence, thereby linking election integrity to platform compliance and rapid mitigation. [32]

## III. LEGAL FRAMEWORK GOVERNING DEEPFAKE-RELATED OFFENCES IN INDIA

The Indian judicial system considers deepfake technology as a criminal offense through various legal instruments which are defined by the BNS 2023 through its offence-mapping system and investigation procedures and through the BNSS 2023 and BSA 2023 and IT Act 2000 and IT Intermediary Rules. The multi-statute approach operates effectively, yet it creates separate legal paths because a single deepfake incident can activate multiple security laws through its impersonation and intimidation and defamation and voyeurism/stalking and public mischief components, while the courtroom evidence process needs to meet electronic-record certification standards and integrity testing requirements. [33]

### *A. Application of Penal Laws to Deepfake-Related Criminal Conduct*

The BNS establishes direct offence connections through s.319 (personation-based cheating) which applies to deepfake fraud and impersonation cases, because document/electronic-record offences emerge when synthetic content functions as a "false" record to deceive, with s.336 (forgery) and s.340 (forged document or electronic record used as genuine) applying as the most relevant offences. The deepfake format shows that s.356 (defamation) defends reputational damage through visible representation which displays false imputations. The s.351 (criminal intimidation) law provides essential protection against blackmail threats because it includes all types of threats which can target people and their possessions and their reputation, while it defines aggravated situations through specific intimidation types, which enables legal

[32] Sparsh Upadhyay, "Reasonable Care Must Be Applied Before Invoking Offence Of Endangering Sovereignty, Unity & Integrity Of..." *Live Law*, 11 July 2025.
[33] Editor, "Emerging Technologies and Law: Legal Status of Tackling Crimes Relating to Deepfakes in India" *SCC Times*, 2023 *available at*: https://www.scconline.com/blog/post/2023/03/17/emerging-technologies-and-law-legal-status-of-tackling-crimes-relating-to-deepfakes-in-india/ (last visited May 10, 2026).

authorities to treat deepfake threats as serious offenses that extend beyond basic online abuse when their purpose is to force people to act or stay silent. [34]

The BNS recognizes privacy and dignity violations through two specific statutes, which include s.77 (voyeurism) and s.78 (stalking), because deepfake abuse through non-consensual sexualized content and digital monitoring create direct harm to victims. The public-order entry point of s.353 establishes a legal framework which protects community threats through its provisions that criminalize electronic distribution of false information which creates public panic or incites violent clashes between different groups. The application of s.152 arises in national-security-adjacent contexts when deepfakes enable secessionist and subversive activities through electronic communication, because it maintains the lawful criticism exception which protects against such activities without committing the crime, which serves a critical function for constitutional protection. [35]

### *B. Role of Information Technology Law in Addressing Digital Manipulation*

The IT Act, 2000 sets the primary legal framework to combat deepfake crimes because most deepfake attacks occur through cyber-enabled activities which include account takeovers and identity theft and phishing attacks and the sharing of sexually explicit synthetic material. The main provisions which operate in practice include s.66C which addresses identity theft and s.66D which deals with computer resource-based impersonation fraud and s.67 and s.67A which protect against electronic distribution and transmission of obscene content and sexually explicit material which are commonly used for deepfake pornography and synthetic intimate videos. The BNS receives this statutory protection which specifically addresses computer resource misuse and electronic publication through its provisions, which assist investigators in understanding both the digital operation of the crime and the resulting human damage.[36]

Intermediary governance has become more crucial because deepfakes can be distributed through platforms which operate independently of the devices used by their originators to disseminate these falsified videos. The Information Technology (Intermediary Guidelines and

[34] Ravi Goyal And Heba Ajaz, "Mitigating Deepfake Threats: How Existing Laws Can Tackle Misuse" *Live Law*, 16 July 2024.
[35] IJLLR Journal, "Section 78 BNS: Cyberstalking, Gender And Digital Evidence In Contemporary India" *IJLLR Journal*, 2026 *available at*: https://www.ijllr.com/post/section-78-bns-cyberstalking-gender-and-digital-evidence-in-contemporary-india (last visited May 10, 2026).
[36] Editor, "Emerging Technologies and Law: Legal Status of Tackling Crimes Relating to Deepfakes in India" *SCC Times*, 2023 *available at*: https://www.scconline.com/blog/post/2023/03/17/emerging-technologies-and-law-legal-status-of-tackling-crimes-relating-to-deepfakes-in-india/ (last visited May 10, 2026).

Digital Media Ethics Code) Rules 2021 which have been updated through newly enacted rules create specific due diligence requirements and compliance standards which intermediaries must follow while their policy documents and advisories require them to manage synthetic content risks. The instruments require deepfake mitigation processes to implement identification through labelling, establish traceability, and develop operational procedures which ensure timely responses to legal requests, which creates consequences for deepfake mitigation efforts before criminal trials reach their final outcomes. [37]

### *C. Limits and Gaps in the Existing Legal Response to Deepfake Crimes*

The penal code creates a major gap because the legal definition of deepfake as an independent crime does not exist which requires determination of legal accountability through existing criminal offenses. The system creates ambiguity when dealing with cases which produce widespread damage to public trust while their guilt remains ambiguous, and synthetic media exists between fake usage and genuine content. The BNS law provides effective legal instruments through its sections 353 and 152 which address public disturbance through electronic distribution of false information and protect national unity through electronic communication. BNS requires investigators to demonstrate both intent and certain thresholds of evidence which will help them avoid excessive limits on legal expression rights.[38]

The first gap exists because deepfakes reach their highest destruction capacity during their initial period which criminal justice systems require more time to resolve. The government advisory system demands different parties to execute content verification procedures which should lead to immediate enforcement actions against synthetic materials. The implementation of procedural standards for notice, takedown, data preservation, and cooperation processes creates essential procedures which face execution challenges when creators, hosting services, and target audiences operate from different regions. [39]

[37] Aayushman Gaikwad & Smruti Mishra, "Three Hours To Comply: India's New Rules For AI-Generated Content And Deepfakes" *Live Law*, 21 February 2026.
[38] Editor, "Emerging Technologies and Law: Legal Status of Tackling Crimes Relating to Deepfakes in India" *SCC Times*, 2023 *available at*: https://www.scconline.com/blog/post/2023/03/17/emerging-technologies-and-law-legal-status-of-tackling-crimes-relating-to-deepfakes-in-india/ (last visited May 10, 2026).
[39] Aayushman Gaikwad & Smruti Mishra, "Three Hours To Comply: India's New Rules For AI-Generated Content And Deepfakes" *Live Law*, 21 February 2026.

### *D. Case laws*

The court case ***Anand Giri @ Ashok Kumar Chotiya v. State of U.P. & Another***[40] establishes its importance through its evidence of pigment to which the defendant used to show no ability to create the false documents through the lack of connection between him and the documented evidence. BNS sections 351, 356 and 336 and 340 provide the legal framework which research needs to examine together with BSA sections 62 and 63(4) to prove the deepfake blackmail cases and the resulting reputation damage which modern society faces today.

The case of ***Mrs. X v. Union of India & Others***[41], contains one of the most important Indian judicial decisions about online intimate-image abuse. The court determined that the petitioner's intimate images which he shared without consent should remain available on the internet because he wanted to use them as proof against others to make them remove the content and stop sharing it. The present legal framework assigns BNS sections 77, 78, 351 and 356 to the described situation, while BNSS sections 173 and 105 govern complaint handling and electronic investigation, and BSA sections 62 and 63(4) determine the methods for testing digital evidence.

The Delhi High Court case ***Anil Kapoor v. Simply Life India & Others***[42], resulted in a prohibition against the defendant's usage of the plaintiff's name, image, voice and persona through Artificial Intelligence and Machine Learning and deepfake technology and face morphing and GIFs for commercial purposes while the court ordered the defendant to block all internet domains and links. This case represents the first Indian legal decision which establishes deepfake technology as a violation of personality rights. The current examination of this behavior through criminal law would create BNS charges which include sections 319, 336, 340 and 356, while IT Act sections 66C and 66D which cover digital platform impersonation will also apply to this situation.

In the lawsuit ***Ananda G @ Ananda Guruji v. Speed News Kannada Media Broadcast Pvt. Ltd., O.S. No. 4103/2021***[43], the plaintiff claimed that the defendant media channel had created a morphed video through deepfake technology and planned to show the video on their channel.

[40] Anand Giri @ Ashok Kumar Chotiya v. State of U.P. & Another, Criminal Misc. Bail Application No. 51323 of 2021
[41] Mrs. X v. Union of India & Others, W.P.(CRL) 1505/2021, 2023: DHC:2806
[42] Anil Kapoor v. Simply Life India & Others, CS(COMM) 652/2023
[43] Ananda G @ Ananda Guruji v. Speed News Kannada Media Broadcast Pvt. Ltd., O.S. No. 4103/2021

The court issued an injunction which prevented the distribution of defamatory content. The analysis of deepfake crimes holds direct relevance to this civil injunction case because the facts demonstrate threats of extortion and reputational damage. The current legal framework establishes BNS sections 351, 356, 336 and 340 as the main applicable laws for this conduct, while electronic distribution activities connect with IT Act section 79 and its rules for online service providers who manage user-generated content.

The High Court recorded the prosecution case in ***Hobin K. K. v. State of Kerala***[44], which presented evidence that the defendant had digitally altered the victim's photos into explicit content while persistently stalking her through digital channels which resulted in severe emotional distress. The current case represents one of the most evident contemporary criminal cases which demonstrate how digital alterations lead to gender-based attacks. The new criminal-law framework establishes the conduct as equivalent to BNS section 77 which defines voyeurism and section 78 which defines stalking and section 351 which defines criminal intimidation and section 356 which defines defamation while the digital files need BSA sections 62 and 63(4) to establish their proof requirements.

The court recorded in ***Kamya Buch v. Jix5A & Others***[45] that the defamatory material extended beyond regular posts to include morphed images and AI-generated visuals and deepfake material and pornographic or nude images and videos which showed the plaintiff in an obscene and malicious manner. The case establishes an essential precedent because it demonstrates how Indian courts currently treat deepfake content as an independent litigation matter. The current BNS legal framework requires application of BNS sections 351, 356, 77 and 78 and IT Act sections 67 and 67A when there is established electronic publication.

The legal case ***Upasana Vohra v. Bee Vitigo & Others***[46], which involved multiple Facebook pages, contained videos that prosecutors said were altered through editing to create a false impression that the plaintiff endorsed medical and wellness products that she had never endorsed. The demonstration of deepfake-style manipulation in this study proves its value for dissertation research because it shows how deepfake-style manipulation creates commercial deception and identity theft. The present legal structure establishes a strong connection between actual events in the case and BNS section 319 which prohibits cheating through personation

[44] Hobin K. K. v. State of Kerala, Bail Application No. 8249 of 2025, 2025: KER:51917
[45] Kamya Buch v. Jix5A & Others, CS(OS) 465/2025
[46] Upasana Vohra v. Bee Vitigo & Others, CS(COMM) 816/2025

and BNS sections 336 and 340 which prohibit false electronic record creation and usage and IT Act sections 66C and 66D which address identity theft and computer-based personation.

The Delhi High Court case ***Mr. Sudhir Chaudhary v. Meta Platforms Inc. & Others***[47], establishes that multiple defendants operated AI-generated and deepfake videos which used the plaintiff's name and image and likeness and voice to generate false content for financial profit which resulted in lost goodwill and credibility. This case serves as the primary legal precedent about false-news deepfakes which use a well-known media figure as their foundation. The current penal system allows BNS sections 319, 351, 353 and 356 to apply to this fact pattern while digital impersonation aspects remain closely linked to IT Act sections 66C and 66D.

The court decision in ***Ranganthan Madhavan v. G Fimlz Studioz and Others***[48], which protected the plaintiff against AI deepfake movie trailer and short video content that used his likeness, established that unauthorized use of personality rights for commercial purposes constitutes an injunctable offense. The order provides essential value because it offers solutions for both deepfake entertainment content and the methods platforms use to remove such content. The BNS sections 319, 336, 340 and 356 now provide criminal-law analysis for conducts which show proof of deception and inducement and reputational damage. Digital file evidence requires BSA section 62 and BSA section 63(4) compliance for its proof and preservation process.

The Delhi High Court handled the ***Swami Ramdev v. John Doe(s) and Others***[49] recorded allegations of an "unprecedented and alarming onslaught of AI-generated deepfake videos, manipulated photographs, impersonating social media accounts, distorted caricatures and fabricated endorsements" across YouTube, Facebook, Instagram, X and e-commerce websites. The Indian legal system permits this document to serve as evidence about how synthetic media is misused across various digital platforms. This dissertation study in criminal justice combines deepfake production with impersonation and fake endorsements and reputational damage and platform distribution which relate to BNS sections 319 and 351 and 356 and 353 and IT Act sections 66C and 66D and 79.

[47] Mr. Sudhir Chaudhary v. Meta Platforms Inc. & Others, CS(COMM) 1089/2025
[48] Ranganthan Madhavan v. G Fimlz Studioz and Others CS(COMM) 1392/2025
[49] Swami Ramdev v. John Doe(s) and Others CS(COMM) 147/2026

## IV. EVIDENTIARY ISSUES IN THE INVESTIGATION AND TRIAL OF DEEPFAKE CRIMES

Deepfake cases require extensive evidence because courts need to determine whether a video has been altered, who is responsible for its creation, who uploaded it, and whether the defendant possessed the necessary intent. The BSA 2023 serves as the framework for electronic evidence through India's new evidence law which directs electronic content proof via BSA s.62 with BSA s.63 providing admissibility rules and certification systems that need a certificate for electronic evidence submission. The focus of deepfake litigation revolves around proving video integrity and provenance because the court needs these factors to establish forensic reliability.[50]

### *A. Challenges in Detection, Authentication and Attribution of Deepfake Material*

Current detection methods face difficulties because current deepfake technology enables fake videos to maintain their authentic appearance while continuing to be used for multiple encoding processes which remove all authenticating evidence from the video. The authentication process requires multiple forensic investigation methods which include analyzing metadata and comparing original files and studying compression patterns and matching biometric data of voices and faces and using platform activity records because all methods need to use evidence which should be stored right away. The BNSS integrity system protects collection integrity through its requirement to document search and seizure events with audio-video electronic procedures which act as proof for maintaining chain-of-custody records about cloned devices. The preservation request along with the initial complaint needs to be considered because deepfake content which exists on cloud platforms can be eliminated instantly or transferred to different locations. [51]

Attribution is usually the hardest step: proving who created the deepfake (not merely who forwarded it) often requires correlating device artefacts (model weights, project files, editing timelines), account access histories, and network evidence. The prosecution needs to demonstrate that investigators used valid methods to collect electronic evidence which connects the defendant to the creation pipeline and then used legal electronic documentation to

[50] Editor, "Emerging Technologies and Law: Legal Status of Tackling Crimes Relating to Deepfakes in India" *SCC Times*, 2023 *available at*: https://www.scconline.com/blog/post/2023/03/17/emerging-technologies-and-law-legal-status-of-tackling-crimes-relating-to-deepfakes-in-india/ (last visited May 10, 2026).
[51] Sonam Singh and Amol Dhumane, "Unmasking digital deceptions: An integrative review of deepfake detection, multimedia forensics, and cybersecurity challenges," 15 *MethodsX* 103632 (2025).

prove this connection. The BSA structure makes this linkage documentation-heavy because each relevant output—hash logs, extraction reports, device images, platform responses—must be packaged for admissibility and reliability assessment under BSA s.63 and its certificate requirements under s.63(4). [52]

### *B. Admissibility and Reliability of Electronic Evidence in Deepfake Prosecutions*

In deepfake prosecutions, courts will typically see multiple "versions" of the same content: a social media re-upload, a screen recording, a forwarded file, and sometimes a recovered original. The BSA resolves admissibility by treating computer outputs as documents when statutory conditions are satisfied, but it also insists on procedural discipline through BSA s.63(4) certificates that identify the electronic record, describe its production, and provide device particulars and compliance statements. The investigators need to create their evidence collection strategy because their evidence collection must satisfy the requirements needed for court acceptance while they need to gather their materials which include original URLs platform timestamps server responses device extraction logs and hash values. [53]

The way electronic records were obtained and stored their storage method and storage duration will determine their reliability. BNSS requires all search and seizure activities to be recorded through audio and video which strengthens procedural credibility by reducing disputes about what was seized when it was seized and whether tampering occurred. The combination of BSA certification and detailed documentation establishes an evidence process that withstands defense challenges which are common in deepfake trials that include allegations of investigator planting evidence and editing devices during processing. [54]

### *C. Burden of Proof, Forensic Difficulties and Investigative Constraints*

The prosecution must provide sufficient evidence for proving the crime charge to the level of absolute certainty because deepfake technology enables defense teams to demonstrate reasonable doubt through their ability to show evidence of fabricated content or misattributed

[52] Editor, "Emerging Technologies and Law: Legal Status of Tackling Crimes Relating to Deepfakes in India" *SCC Times*, 2023 *available at*: https://www.scconline.com/blog/post/2023/03/17/emerging-technologies-and-law-legal-status-of-tackling-crimes-relating-to-deepfakes-in-india/ (last visited May 10, 2026).
[53] Rohit Patel, "Me, Myself and AI: Chasing Deepfakes Across Borders Without Losing Your Rights" *SCC Times*, 2025 *available at*: https://www.scconline.com/blog/post/2025/11/08/deepfake-regulation-rights/deepfake-regulation/ (last visited May 10, 2026).
[54] Justice Narayana Pisharadi, "Recording Of Search And Seizure Through Audio-Video Electronic Means Under Section 105 Of The BNSS" *Live Law*, 19 January 2025.

material or modified content by unidentified third parties. The investigation faces substantial challenges because it requires complete forensic resources and time to complete all investigations because any delay in obtaining system logs or improper device imaging will result in evidence weakening. The BNSS established system which tracks electronic records and documented property seizure operations enables organizations to monitor their initial operational processes which they can later verify through judicial proceedings. The electronic communication system of BNSS section 173 enables organizations to provide information about cognizable offences through electronic communication which results in quick investigation start and evidence retention. The section 105 of BNSS establishes fixed procedures which police departments must follow during their evidence collection activities.[55]

Investigative constraints are also institutional: forensic labs may have limited deepfake detection tooling; police stations may lack trained personnel; and cross-platform evidence requests may be slow. The prosecution uses various pieces of digital evidence which includes account ownership and device possession and editing artefacts and payment traces and communication records to build its case because BSA section 63 requires all evidence to exist as valid electronic records. The legal standard requires proof of deepfake creation but the prosecution must demonstrate authentic proof which links the creator to the material through valid electronic documents.

## V. INSTITUTIONAL RESPONSE AND CRIMINAL JUSTICE CHALLENGES

The enforcement of deepfake technology requires five interconnected steps which start with police officers taking reports and end with courts handling electronic evidence conflicts. The BNS system provides various ways to charge an offender yet its success depends on conducting investigations which follow BNSS standards and BSA rules for proof collection and on using IT systems to achieve rapid evidence elimination and data protection. The ability of institutions to function determines whether legal systems work on actual cases or stay inactive because of their internal deficiencies.[56]

[55] Gagan Verma & Mahima Wahi, "Deepfakes, Due Diligence And The Good Samaritan Paradox; How India's 2026 IT Amendment Rules Resolve..." *Live Law*, 15 April 2026.
[56] Abhay Anturkar, "Deepfakes And Dignity: The New Battle For Celebrity Rights In India" *Live Law*, 27 November 2025.

### *A. Role of Police, Cyber Cells and Forensic Agencies in Deepfake Cases*

Police officers together with cyber cells need to identify the case type which they need to investigate because the incident requires them to decide between six charging options which include impersonation fraud and other criminal activities. The decision establishes various actions which include device confiscation and platform data requests and evidence protection. The BNSS system permits organizations to execute their operations through two specific provisions which include section 173 which allows electronic information transfer about serious crimes and section 105 which permits audio-video documentation of search operations which will enhance operational efficiency when dealing with uncertain evidence and vindicates against evidence tampering claims. [57]

Forensic agencies serve as gatekeepers because they require expert validation which declares evidence as either synthetic or altered and they need dedication that links the material back to the defendant to permit court proceedings. Deepfake analysis needs multiple tools because it requires constant updates to match the fast changes in generative technology which research facilities need modern detection systems and audio-visual file management procedures and judicial reporting methods that courts need to assess. The BSA framework requires organizations to implement structured reporting because BSA s63(4) establishes documentation and certificate-based electronic records as essential proof requirements that transform forensic reports into validated evidence which must maintain its original state for future assessments. [58]



### *B. Procedural Difficulties in Prosecution, Trial and Victim Protection*

The criminal process needs time to proceed through its stages but victims face immediate damaging effects which include loss of reputation and mental suffering and their anxiety about potential information leaks. The urgent need for victims to remove content and stop re-uploading is essential for their protection even when BNS sections s.351 (threats) and s.356 (defamation) apply. The government has consistently warned that intermediaries must fulfill their due diligence requirements which the IT Act and IT Rules establish to prevent the spread

[57] Shubhi, "Maharashtra Audio-Video Electronic Means Rules 2026 notifie" *SCC Times*, 2026 *available at*: https://www.scconline.com/blog/post/2026/01/28/maharashtra-notified-audio-video-electronic-means-rules-2026/ (last visited May 10, 2026).

[58] Christian Kraetzer et al., "Process-Driven Modelling of Media Forensic Investigations-Considerations on the Example of DeepFake Detection," 22 *Sensors (Basel, Switzerland)* 3137 (2022).

of synthetic content because the government depends on platform control to minimize damage during criminal investigations.[59]

The defence team uses admissibility tests to evaluate electronic evidence which includes two components: verifying the record's certification and examining the chain-of-custody and the capture evidence for potential content changes. BSA s.62–63 holds essential importance because BSA s.63(4) requires certification whenever authorities submit evidence. BNS prosecutors must construct a consistent narrative that links all elements of the crime together with their valid digital evidence. The BNSS procedures at s.105 enable officials to establish evidence of seizure through official documentation but the system requires both prosecutorial and judicial understanding of technical evidence so cases can proceed without delays and without losing cases through court procedural failures. [60]

### *C. Judicial, Administrative and Regulatory Barriers in Effective Enforcement*

Judicial barriers often arise from technical asymmetry judges need to determine material reliability which requires advanced technical expertise yet they must maintain trial proceedings. For deepfake disputes to achieve standardized court results, institutional support through trained court personnel and forensic report templates and standardized BSA electronic evidence regulations needs to be implemented. The administrative process becomes complicated because states need to collaborate with cyber units and forensic labs, particularly when deepfake incidents reach across multiple jurisdictions with different intermediaries using various methods. The BNSS system needs documented procedures while the BSA system requires structured evidence rules because they ensure deepfake cases remain ready for trial.[61]

The development of platform obligations shows the presence of regulatory barriers which currently exist in the industry. The IT Rules regime now requires stronger enforcement through its updated requirements, but this enforcement depends on three factors: obligation clarity, detection and labelling technical possibilities, and standard procedures for lawful requests and user notifications and transparency measures. The establishment of election integrity rules,

[59] Shreya Saraiya, "Victim Participation In Criminal Justice System: An Indian Perspective" *Live Law*, 13 December 2022.
[60] Bhumika Indulia, "Electronic Evidence in Focus: Navigating Legal Shifts in the Law on Electronic Evidence under the BSA, 2023" *SCC Times*, 2024 *available at*: https://www.scconline.com/blog/post/2024/10/23/electronic-evidence-in-focus-navigating-legal-shifts-in-the-law-on-electronic-evidence-under-the-bsa-2023/ (last visited May 10, 2026).
[61] Amisha Shrivastava, "Use Of AI-Generated Fake Judgments : Supreme Court Urges BCI To Form Expert Panel To Examine Issue" *Live Law*, 5 May 2026.

which include ECI guidelines for synthetic political content labelling, shows how governments now choose to manage their systems through active preventive measures. Criminal enforcement needs platforms to deliver evidence and attribution information, which they can only do when their compliance systems reach full operational status.[62]

## VI. CONCLUSION AND RECOMMENDATIONS

### *A. Conclusion*

The Deepfake crimes which occur in India create a fundamental conflict because the existing BNS 2023 offense categories enable the legal system to identify damage through legal recognition but the system requires strong electronic-evidence discipline and institutional capacity for fast and accurate proof evaluation. The most usable offence anchors for deepfake harm remain BNS s.319 (impersonation-based fraud), s.336 and s.340 (forgery and use of forged electronic records), s.351 (criminal intimidation), s.356 (defamation), s.77–78 (voyeurism and stalking), s.353 (public mischief via electronic falsehoods), and in higher-stakes influence operations, s.152 (endangering sovereignty/unity via electronic communication). The provisions of these laws function properly only when investigations and trials follow BNSS procedural integrity standards which include s.173 and s.105 and BSA electronic evidence admission standards which include s.63(4) certification requirements.

### *B. Recommendations*

1. India should establish standardized protocols for deepfake investigations which should follow BNSS s.105 regulations concerning audio-video search and seizure recording. The trial evidence capture system should operate as a complete solution for prosecutors who need to achieve BSA s.63(4) certification requirements without needing to conduct evidence reconstruction procedures.
2. Capacity-building needs to receive priority through establishment of dedicated deepfake detection units which will function inside cyber cells together with their establishment of accredited forensic workflows and their provision of training programs for prosecutors about electronic record admissibility according to BSA ss.62–63.

[62] Dipika Jain, "Regulation of Digital Healthcare in India: Ethical and Legal Challenges," 11 *Healthcare (Basel, Switzerland)* 911 (2023).

3. Victim protection should be implemented through fast coordination with intermediaries who handle preservation requests which use due diligence standards from the IT framework while BNS criminal proceedings continue.
4. Synthetic content regulations during elections need to become stricter through the creation of mandatory labeling requirements which will hold parties accountable according to ECI guidelines and the new IT Rules framework while maintaining evidence-based enforcement that matches its level of enforcement.

*******

**References**

**Statutes**

1. The Bharatiya Nyaya Sanhita, 2023
2. The Bharatiya Nagarik Suraksha Sanhita, 2023
3. The Bharatiya Sakshya Adhiniyam, 2023
4. The Information Technology Act, 2000
5. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
6. The Digital Personal Data Protection Act, 2023

**Books**

1. Talat Fatima, *Cyber Law in India* (Kluwer Law International, Alphen aan den Rijn, 2017). *available at*: https://law-store.wolterskluwer.com/s/product/cyber-law-in-india/01t0f00000J3ambAAB?srsltid=AfmBOoptYyYELvFJbNypRHMBQvPkgcEn6ksO7GGlfTqj7L0rGojKxcc7
2. Nayan Joshi, *Electronic Evidence* (Eastern Book Company, Lucknow, 2nd edn., 2025). *available at*: https://www.ebcwebstore.com/product/electronic-evidence-nayan-joshi-2nd-edition?products_id=99110142&srsltid=AfmBOoq-Icju7cLhLGEuntbd3NE8AWvEI1jqVvKs2MArZQIzJgW_WHEu
3. Purvi Pokhariyal, Amit K. Kashyap and Arun B. Prasad, *Artificial Intelligence: Law and Policy Implications* (Eastern Book Company, Lucknow, 2024). *available at*: https://www.ebcwebstore.com/product/artificial-intelligence-law-and-policy-implications-by-purvi-pokhariyal-amit-k-kashyap-and-arun-b-prasad?products_id=99097334&srsltid=AfmBOooeBL3kYoM-M_6iqcqzUymWpdvBHoT8SG9wmBg78R7fbhror5Dp
4. Thomas D.C. Bennett and Rebecca Moosavian (eds.), *Deepfakes and the Law: Challenges, Responses, and Critique* (Routledge, London, 2025). *available at*: https://www.routledge.com/Deepfakes-and-the-Law-Challenges-Responses-and-Critique/Bennett-Moosavian/p/book/9781032964539
5. Edward J. Swan, *Artificial Intelligence Law* (Kluwer Law International, Alphen aan den Rijn, 2024). *available at*: https://www.adityabooks.in/details/artificial-intelligence-law/13267

**Journals**

1. Jyothsna Gurumurthy, "In the Pursuance of a Robust Legal Framework to Address Deepfake Harms: An Analysis of the Indian Legal Discourse," 20 *Indian Journal of Law and Technology* 1 (2024). *available at*: https://repository.nls.ac.in/ijlt/vol20/iss1/1
2. Shimona Mohan and Sarthak Wadhwa, "Deepfakes and Shallow Laws: Regulating Distorted Narratives in the Political Cyberspace," 19 *Indian Journal of Law and Technology* 94 (2023). *available at*: https://repository.nls.ac.in/ijlt/vol19/iss2/4
3. Maria-Paz Sandoval, Maria de Almeida Vau, John Solaas and Luano Rodrigues, "Threat of Deepfakes to the Criminal Justice System: A Systematic Review," 13 *Crime Science* 41 (2024). *available at*: https://link.springer.com/article/10.1186/s40163-024-00239-1
4. Felipe Romero-Moreno, "Generative AI and Deepfakes: A Human Rights Approach to Tackling Harmful Content," 38 *International Review of Law, Computers & Technology* 297 (2024). *available at*: https://www.tandfonline.com/doi/full/10.1080/13600869.2024.2324540
5. Tyrone Kirchengast, "Deepfakes and Image Manipulation: Criminalisation and Control," 29 *Information & Communications Technology Law* 308 (2020). *available at*: https://www.tandfonline.com/doi/abs/10.1080/13600834.2020.1794615
6. Alex Barber, "Freedom of Expression Meets Deepfakes," 202 *Synthese* art. 40 (2023). *available at*: https://link.springer.com/article/10.1007/s11229-023-04266-4
7. Bao Kham Chau and George He, "Audio Deepfakes and the Regulation of the Landlords of Creativity," 1 *Cambridge Forum on AI: Law and Governance* e30 (2025). *available at*: https://www.cambridge.org/core/journals/cambridge-forum-on-ai-law-and-governance/article/audio-deepfakes-and-the-regulation-of-the-landlords-of-creativity/384CF445141FBA75B697198CF310D453
8. Noelle Martin, "Online Safety Regulation of Deepfake Abuse: A Case Study on Australia's eSafety Commissioner," 34 *Griffith Law Review* 23 (2025). *available at*: https://www.tandfonline.com/doi/full/10.1080/10383441.2025.2504791
9. Parkhi Saxena and Gaurav Pathak, "Deepfakes, Big Tech, and Human Rights Challenges: Examining the Technology from a Feminist Legal Lens," 29 *The International Journal of Human Rights* 1 (2025). *available at*: https://www.tandfonline.com/doi/abs/10.1080/13642987.2025.2602137
10. Priyansh Nema, "Deepfakes in India," 29 *International Journal of Law and Information Technology* 1 (2021). *available at*: https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals%2Fijlit29&section=19

*******