Page: 452-471 *URL: www.lijdlr.com*

LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

ISSN: 2583-7753

LawFoyer International Journal of Doctrinal Legal Research

[ISSN: 2583-7753]

Volume 3 | Issue 4

2025

DOI: https://doi.org/10.70183/lijdlr.2025.v03.139

THREAT OF DEEPFAKES AND INDIAN CRIMINAL LAW'S ADEQUACY TO ADDRESS THE EMERGENT NEED FOR PROTECTIONS

Aditi Pandey[1]

I. ABSTRACT

This paper addresses the growing threat of AI-enabled crimes, particularly deepfakes and identity intrusion, which jeopardize the right to privacy, reputation, and public order. It examines the adequacy of existing Indian legal frameworks, including the Bharatiya Nyaya Sanhita and the Information Technology Act, in providing recourse and remedies to victims. The proliferation of generative AI technologies has made it increasingly easy to create hyper-realistic synthetic media that can deceive viewers, manipulate public opinion, and cause irreparable harm to individuals and institutions. From non-consensual intimate imagery targeting women to political disinformation campaigns designed to influence elections, deepfakes present multifaceted challenges that existing laws were not designed to address. This paper critically evaluates key provisions under the BNS 2023, including those related to forgery, defamation, criminal intimidation, and sexual offenses, alongside relevant sections of the IT Act 2000 concerning identity theft, impersonation, and obscene content as well as absence of deepfake-specific legislation, the paper further analyzes global legal responses to such crimes and proposes reforms tailored to the Indian context to bridge the identified legislative and enforcement gaps.

II. KEYWORDS

Deepfakes, Bharatiya Nyaya Sanhita (BNS) 2023, Information Technology Act 2000, AI-generated content, Non-consensual pornography, Cyber law India, Digital forgery, Personality rights

[1] LLB 2nd Year Student at lloyd law college (India). Email: aditipandeyofficial@gmail.com

 (ISSN: 2583-7753)

III. INTRODUCTION

Deepfakes, which are realistic synthetic images, videos, or audio recordings that show actual people saying or doing things they never did, have been made possible by the development of generative AI. Such material can readily support scams, non-consensual pornography, and misinformation, eroding public confidence and individual reputations. "Deepfakes can proliferate, causing uncertainty, and tarnish public and personal reputations before fact-checking and law enforcement can act," according to a recent analysis. Incidents involving false pornographic movies featuring celebrities and AI-generated political "propaganda" have already surfaced in India, highlighting the need for legal readiness.

The new Bharatiya Nyaya Sanhita, 2023 ("BNS") took the place of the British-era IPC and went into force on July 1, 2024. The BNS seeks to update and "Indianize" penal laws in order to address current concerns. It does not, however, directly name "deepfakes" or AI-related offenses. Instead, existing violations (including impersonation, forgery, defamation, and obscene content) are reframed using the current phrasing. This article asks if the issues surrounding deepfakes can be adequately addressed by the BNS and other Indian laws. In other words, where do Indian criminal and civil laws fall short in their mapping of deepfake behavior?

First, we examine the BNS provisions—such as those on false evidence, electronic record forgery, defamation, harassment, privacy, etc.—that may be connected to deepfakes and contrast them with the corresponding IPC sections. We next examine additional legislation, including data protection/privacy law, election regulations, and the Information Technology Act 2000 (specifically, Sections 66C, 66D, and 66E on identity theft/impersonation/privacy and 67–67B on obscene electronic content). Next, we take into consideration public occurrences, FIRs, and reported cases involving deepfakes in India, as well as the reactions of the courts and law enforcement. Following an overview of legal remedies (criminal charges, injunctive relief, civil claims, and procedural tools for digital evidence), we address any remaining gaps, including the lack of a specific

deepfake offense, issues with jurisdiction and anonymity, authentication challenges, and gender/political ramifications.

IV. AN ANALYSIS OF BNS 2023/IPC PROVISIONS POTENTIALLY RELATED TO DEEPFAKES

When a deepfake is used to deceive or cause injury, its prohibitions on false evidence, impersonation, forgery, defamation, sexual privacy, and harassment are especially important. Notably, there is no distinct "deepfake" offense created by the BNS. Instead, acts that may employ deepfake technology are now covered by existing offenses.

A. Forgeries and False Evidence

Deepfakes may be considered fake evidence. False evidence is covered in Chapter XIV of BNS. "Fabricating false evidence" is defined in Section 228 as creating any document or item with the intention of skewing legal or administrative procedures. Making a deepfake video in order to fraudulently implicate someone would be considered a qualifying act. False evidence is punished by the BNS: Giving false testimony with knowledge can result in up to seven years in prison, according to Section 229(1). Section 231 deals with providing or creating false evidence in order to convict someone of a major offense (such as a criminal carrying a life sentence) and imposes the same penalty as that crime. Similarly, using evidence that is known to be false is illegal under Section 233. In conclusion, these provisions enable the prosecution of the person who created the deepfake video as well as anyone who intentionally spreads it, should it be presented in court or used as evidence in public.

Crucially, the BNS is able to identify digital and online forgeries. Forging or counterfeiting a document or electronic record is covered under Section 336 (Chapter III: False Evidence and Related Offenses). Forging any "document or electronic record," including pictures or videos, is expressly prohibited. Since creating or altering a fake video is effectively forging an electronic record, this clause has a direct bearing on deepfakes. If the falsified record is used to cheat or damage someone's reputation, the

penalties under Section 336 also increase. Essentially, under BNS, making a malevolent deepfake, particularly to deceive or defame someone, might be considered forgery. "Creating or altering digital photos to distort reality fits [Section 336's] description," according to one remark.

These clauses are equivalent to previous IPC sections. While BNS 336 addresses "electronic record" forgery, IPC forgery (Sections 463–471) does not specifically address electronic records. IPC Sections 463–477 (forgery in legal procedures) and 477A (falsification of accounts) are replaced by Section 228 et seq. of the BNS, which broadens its application to digital content. To put it briefly, BNS gives the law the ability to identify deepfake production as an instance of electronic forgery and to target evidence fabrication through all channels, including AI-generated media.

B. Reputation and Defamation

A person's reputation is frequently the target of deepfakes. Section 356 is the BNS crime of defamation, which punishes making or disseminating any imputation (via words, signs, or outward manifestations) about an individual that damages that person's reputation if the maker meant or thought it would do so. Notably, digital and verbal forms are covered by Section 356. The chapter title is "Defamation by electronic means," and there is no differentiation for online publications. Although BNS utilizes more contemporary wording, this provision is similar to IPC Sections 499–500. (An official table indicates that BNS 356 is equivalent to IPC 499–500.)

Therefore, under BNS, a deepfake image or video that inaccurately depicts someone in an unfavorable light—for instance, by suggesting unlawful or immoral behavior—may be prosecuted with defamation. "Section 356... makes spreading defamatory content via digital media unlawful," according to one analysis, which includes reputation-damaging deepfakes.

Threats that could go along with a deepfake are covered by another crime, criminal intimidation. In general, Section 351 defines intimidation as threatening harm to

someone's body, reputation, or property in order to instill fear or compel them to do action. Section 351 may be applicable if the offender utilizes a deepfake, such as threatening to release a phony degrading video. In fact, Section 351 is highlighted in the VIF research on deepfakes as the BNS counterpart of the IPC's intimidation.

Threatening someone to get false evidence (a form of incentive to mislead investigations) is punishable under a similar Section 232. This could be used to intimidate a court or witness by presenting a deepfake. Deepfake behavior can be prosecuted under a variety of reputation-related offenses under BNS, including defamation, intimidation, and forgery.

C. Sexual Offenses, Consent, and Privacy

Intimate stuff or private people are frequently featured in deepfakes. Non-consensual deepfake porn may be captured by the BNS's privacy-protective sexual offenses. Chapter XI, Sections 75–77, addresses voyeurism, sexual harassment, and assault. Sexual harassment is defined in Section 75 as unwanted physical approaches, sexual statements, or coerced exposure to pornography.

In particular, Section 77 penalizes "whoever watches, or captures the image of, a woman engaging in a private act in circumstances where she expects privacy" in order to combat voyeurism. Although Section 77 was first created for covert photography, it might be argued that it covers any unapproved portrayal of a private sexual act. This ban might apply to a deepfake that shows a woman in a sexual or private setting, even if it was created by artificial intelligence. The BNS statement affirms that taking and sharing women's private photos is covered by Section 77.

A new stalking offense established by Section 78 involves "monitoring" someone's internet activity or maintaining constant contact; this may be relevant if deepfakes are employed in a pattern of harassment. An offense similar to IPC 509 (insulting a woman's modesty) is maintained by Section 79. Although enforcement may be challenging if AI-generated faces make it more difficult to distinguish between "victim" and "actor," these

sexual privacy protections improve protection for victims of non-consensual sexual deepfakes.

D. Additional Offenses (Harassment, Cheating, etc.)

Computer-related offenses are still covered by the IT Act; the BNS does not have a separate "cybercrime" chapter. Nonetheless, a few generic offenses can be relevant. For example, impersonation cheating (IPC 417–418) may now fall under the BNS's fraud and forgery sections. Deepfakes may be prosecuted for fraud and deception if they are employed in a confidence trick (such as displaying a phony CEO video to approve funds).

Additionally, general crimes like public mischief (Section 353, which punishes utterances that cause public disorder) are still included in the BNS. A deepfake intended to provoke panic or violence within a community could be prosecuted under 353(1) (or 353(2) if there is animosity between groups). With updated terminology that includes electronic media, these take the place of IPC 505/506A.

V. IPC VS. BNS COMPARISON FOR RELEVANT OFFENSES

The BNS largely follows the framework of the IPC, however it adds new offenses and updates the phrasing.

Important modifications:

- **Defamation (IPC 499/500 now BNS 356):** The penalties in BNS 356 are substantially the same as those in IPC 499/500. Though it now specifically covers digital publication, the law still needs intent or injury.
- **IPC 463–477 now BNS 228–242, 336 False Evidence/Forgeries:** BNS extends this to specifically address "electronic records" and online settings. For instance, BNS Section 336, which is not included in the IPC, equates the forgery of a digital document with the forgery of any "electronic record." There were no overt stalking or voyeurism offenses under the IPC. BNS presents voyeurism (77) and

stalking (78) from scratch. These filled up the technological gaps for harassment that were not covered by the IPC.

- **Sexual assault:** IPC 354A, 509, and obscenity IPC 292–294 are two examples of sex offenses that are recast by BNS (e.g. sexual harassment in 75, assault to outrage modesty in 76, and insulting modesty in 79). The BNS's traditional IPC obscenity offenses (Sections 292–294), which cover pornographic publications in general, are essentially unaltered. Nonetheless, online obscenity is particularly covered by the IT Act (explained below).
- **Threats and Intimidation:** BNS 351 has replaced IPC 503 (criminal intimidation). The idea behind Section 351, which addresses threats to property, people, or reputation, is precisely the same. Additionally, anonymous threats and kidnapping with threat are expressly illegal under the BNS.

In conclusion, BNS maintains offenses that are applicable to deepfake behavior and, in certain situations, expands them to better suit the digital era. But it doesn't specifically address artificial intelligence or synthetic media anywhere. Interpreting these general offenses in the context of modern technologies will be necessary for enforcement.

VI. ADDITIONAL RELEVANT LAWS

Other laws, such as those pertaining to electoral law, cyber law, intellectual property, and privacy, handle deepfakes from diverse perspectives, while the penal code (now BNS) serves as the foundation for criminal penalties.

A. The Information Technology Act of 2000

The main laws governing computer-enabled crimes and content regulation are found in the IT Act 2000 (as modified).

A number of areas are specifically pertinent to deepfake situations:

- Anyone who "fraudulently or dishonestly makes use of the electronic signature, password, or any other unique identification feature" of another person is

subject to penalties under Section 66C, which deals with identity theft. This clause might apply to deepfake video impersonation that uses someone else's image or digital ID.

- Cheating on a computer by impersonating someone else is punishable under Section 66D (cheating by personation). It may be charged as cheating by impersonation if a deepfake video is used to trick viewers into believing it is an authentic speech or endorsement.
- It is illegal to "capture, publish, or transmit the image of a private area of any person" without that person's agreement, according to Section 66E (privacy). Although voyeurism was its initial target, deepfake pictures of nudity could also be included if they are distributed without permission.
- Section 67 prohibits the publication or transmission of "obscene" content and carries a maximum sentence of three years in prison. Section 67B makes it illegal to show children engaging in sexual activity, whereas Section 67A targets "sexually explicit" content. These provisions would be broken by deepfake pornography, particularly when it involves kids or is not consenting. Therefore, the IT Act offers cyber-specific measures for prosecuting people who post gore or deepfake porn online.

The government can require intermediaries to restrict content that jeopardizes public order, security, or sovereignty under Section 69A, which gives it blocking power. Similar blocking orders have been used by Indian authorities for other harmful content; 69A orders may be triggered by deepfake films that incite violence. Platforms are required by the IT Act to swiftly delete such banned content.

Online intermediaries (social media, ISPs) are granted safe harbor under Section 79 (intermediary liability) if they exercise due diligence. When platforms learn of illegal content or receive a complaint from a user, they must remove it. Once a deepfake has been reported, it must be removed otherwise the platform may lose its protection. This

obligation is reinforced by recent rules (see below), particularly for synthetic media. To put it briefly, the IT Act does not define "deepfakes," but it does establish a partial legal framework through its rules on identity theft, privacy, obscene content, and platform duties.

According to one research, while Sections 66D and 66E are the "closest" legislation currently in place to handle privacy violations and AI impersonation, they "are not enough" to completely address deepfakes. While drafting new legislation, the government has relied on these portions as a stopgap measure. For instance, social media intermediaries were specifically directed to identify, flag, or delete deepfake or misleading content in a government advisory issued in November 2023. It required that reported deepfakes be removed as soon as possible (within 36 hours of notification), stating that failure to do so could result in punishment under the IT Act.

B. Data security and privacy

Despite the Supreme Court's recognition of privacy as a fundamental right under Article 21, India does not currently have a specific "right to privacy" law. The Digital Personal Data Protection (DPDP) Act 2023, which went into effect in 2023, partially covers the misuse of personal data in practice, such as deepfakes. The DPDP Act grants people control over their data and governs how personal data is processed. A malevolent actor may be breaking data protection laws if they use someone else's image to train an AI model (e.g. processing without consent or for a "sensitive personal data" reason).

Theoretically, a victim of unlawful use of their image could seek remedies under DPDP as violations can result in fines and compensation. Nevertheless, DPDP enforcement is still in its infancy, and its suitability for generative AI has not yet been established. Although DPDP is mentioned in the VIF report on deepfakes, no deepfake-specific DPDP action is mentioned. This is probably because DPDP's regulations are still being developed. Overall, data protection lacks criminal fangs but offers an emergent civil remedy through DPDP sanctions.

There is other privacy-related legislation in India, such as the Cable TV Act's banning of pornographic films, but none that specifically addresses AI content. Currently, "privacy" considerations against deepfakes are based on the aforementioned criminal/statutory provisions (e.g. 66E, 77 BNS) and general rights (Article 21).

C. Personality Rights and Intellectual Property

A person's likeness is frequently misused in deepfakes. India does not have a separate "right of publicity" law. In reality, victims have used copyright and trademark/passing-off laws to prevent illegal use of their voice or picture. For instance, the court issued an order against Warikoo in Ankur Warikoo v. John Doe (Delhi HC, May 2025) after deepfake videos exploited his image to demand money. The plaintiff claimed that his registered trademark "Warikoo" had been violated and that his character had been exploited without authorization. The court ordered social media companies to remove these deepfakes as soon as possible, acknowledging that they may be stopped by applying intellectual property principles.

In a related case, the Delhi High Court determined that the use of deepfake AI to illegally superimpose actor Anil Kapoor's picture on pornographic movies met the requirements for injunctive relief. The court awarded remedy on the grounds of passing-off, breach of Kapoor's privacy and personality rights, and copyright (his public pictures). Therefore, Indian courts have permitted celebrities to shield their "name, image, voice, or likeness" against deepfake exploitation even in the absence of legislative rights of publicity.

Regarding copyright, a recent US law (the No AI Fraud Act) defined likeness as an individual's intellectual property; however, India's Copyright Act does not protect an individual's picture unless it is connected to a creative work. While "screenshot" faces are typically uncopyrighted, deepfakes may violate copyright if they use music or a movie clip that is protected by copyright. If a deepfake deceives by using a logo or brand identification, trademark law may be applicable. In general, in addition to criminal charges, victims may combine claims from IP and torts (defamation, misappropriation) to achieve civil remedies (damages, injunctions).

D. Political Speech and Election Laws

Because they allow for targeted propaganda, deepfakes are especially dangerous during elections. Deepfakes are not specifically forbidden by Indian election legislation (the Representation of People Acts, 1950/51). Sec. 125A of the RP Act prohibits intentionally making false representations regarding a candidate's conduct or character, and the Model Code of Conduct (MCC) prohibits inducements and misleading promises. One could argue that a deepfake alleging a politician said anything disparaging might be against Section 125A, which punishes making false statements to sway votes. Section 125A, on the other hand, is limited to misleading assertions regarding character rather than events or policy. The MCC and general criminal laws pertaining to obscenity and defamation may also be applicable.

In reality, courts and the Election Commission of India (ECI) have used interim measures to combat deepfakes. Pre-election rules on deepfakes were demanded by petitioners in a May 2024 PIL before the Delhi High Court. Because "the existing legal framework encompassing both civil and criminal law is fairly insufficient" to address deepfake harms, the Court declined to step in mid-poll. Petitioners were instructed to lodge grievances with ECI. In response, the ECI issued instructions to parties and started a "Myth vs. Reality" registry, which dispels false information. The ECI banned political parties from disseminating "deep fake audios/videos" or false information in May 2024 and mandated that they take down any such content within three hours of being notified.

Regulators have therefore acknowledged the concern, even if there isn't an election crime specifically related to deepfakes. By requiring parties to respond quickly, the ECI's guidelines (as well as pilot initiatives like the Myth Reality portal) supplement legislative measures. In addition to triggering actions under the IT Act (false information creating public mischief, etc.), a deepfake that targets an election may also be considered a violation of Sec. 125A if it falsely damages a candidate's reputation. Enforcement, however, is case-by-case and reactive, much like general speech restriction.

VII. CURRENT DEEPFAKES CASES AND INCIDENTS

A number of real-life occurrences in India demonstrate how deepfakes have influenced public opinion and prompted legal reactions.

A. Political Disinformation

Gujarat Police reported a person from Delhi who shared a deepfake video of Union Finance Minister Nirmala Sitharaman in July 2024 under Sections 500 (defamation) and 505(2) (communal hatred) of the IPC. Regarding the Goods and Services Tax, the FM was misquoted in the video as referring to it as the "Gopaniya Suchna Tax."

Local authorities called the act "abhorrent," and the anonymous uploader on Twitter/X was the subject of an arrest warrant. Similar to this, in May 2024, the Mumbai Cyber Police reported a deepfake video purporting to show Home Minister Amit Shah saying the BJP would eliminate reservations for SC, ST, and OBC.

The BJP leader who filed the complaint drew attention to the inconsistency with Shah's actual remarks. To file the complaint, the police used the IPC's anti-enmity and anti-impersonation sections. These instances demonstrate how authorities use current laws to prosecute offenders and see deepfake videos as being on par with defamation and disinformation.

A cyber complaint made by a political leader: The public was outraged when a West Bengal CPM youth leader filed a cybercrime complaint in May 2025 over an "AI-generated manipulated photograph" that purportedly showed him meeting a suspected Pakistani spy. AI produced the image by substituting the politician for the real person. Following the complaint, Kolkata police reportedly filed a formal case. This demonstrates police willingness to regard AI-manipulated photographs as actionable cyber offenses, even though it is not a court case.

B. Celebrity Cases

In response to deepfake abuse of their personas, celebrities have started to ask the courts for remedy. YouTuber Ankur Warikoo was granted a John Doe injunction by the Delhi High Court in May 2025. On social media, deepfake films purporting to show him supporting phony stock-tips schemes had targeted him. The court ruled that these AI-generated impersonations infringed against Warikoo's trademark and publicity rights, and it prohibited anonymous parties from using his name, image, or voice in any way, including deepfake or AI.

Within 36 hours, Meta (Facebook/Instagram) was required to remove the offensive videos. In a different instance, Bollywood star Anil Kapoor was granted a similar injunction in 2023 after unidentified parties utilized artificial intelligence to overlay his face on pornographic movies in order to promote services. A prima facie case of harm to Kapoor's reputation and character was determined by the Delhi Court. These rulings are enforced through temporary injunctions and are primarily based on passing-off and intellectual property grounds (with a focus on privacy). They highlight the readiness of courts to prevent deepfakes through equitable remedies.

C. Public Figures and Media

In addition to courts, fact-checkers and social media platforms have identified deepfakes. For example, in 2024–2025, a widely shared AI-manipulated image purportedly showing Congress leader Rahul Gandhi in a compromising pose with a journalist (Jyoti Malhotra) went viral. It was refuted by fact-checkers as a "manufactured" image. The instance shows how media attention and public knowledge are the first line of defense against deepfakes, even though no formal complaint is filed. (It also draws attention to the dangers of slander, since public personalities like Gandhi have reputations to preserve.)

These instances demonstrate how authorities respond to each issue by utilizing the laws that are available (IPC, IT Act, and personality rights). However, because BNS is new, we do not discover any documented convictions expressly under BNS. Up to the middle of

2024, the majority of enforcement has depended on the IPC/IT Act. However, the legal changes are important for the framing of future cases (see the next sections).

VIII. LEGAL RECOURSE AND THE VICTIMS' PROCESS

Although there are real barriers, Indian law provides victims of damaging deepfakes with both criminal and civil remedies.

A. Criminal Redress

According to the applicable criminal provisions, a victim may submit a police complaint (FIR).

For instance:

- **Defamation:** The victim may file a complaint under IPC Section 499 (soon BNS 356) if they are slandered by a deepfake video. For producing or disseminating the defamatory deepfake, a formal complaint may be filed. (Online defamation is usually considered a crime under police rules, and victims frequently file false information reports under IPC 500).
- **Cyber Offenses:** This is supplemented by the IT Act. If a deepfake involves the misuse of a victim's identity, the victim may file a complaint under IT Sections 66C/D/E (identity theft or cheating by impersonation). Under Section 67/A/B, they can also file a complaint against pornographic deepfakes.
- **Harassment or Obscene Material:** IPC/BNS sexual offence provisions (e.g., 354A, 509; or BNS 77 voyeurism, 79 modesty) may be used if a deepfake contains sexual content of a woman without her agreement. A women artificially produced pornography, for example, would be considered "publication of obscene matters."
- **Threats/Intimidation:** The criminal intimidation (IPC 503/BNS 351) or blackmail laws may be applicable if deepfakes are employed for extortion or blackmail.

- **Public Mischief/Incitement:** BNS 353 may be used to prosecute a deepfake that causes unrest in the community.

The police conduct an investigation after a formal complaint is filed. Digital forensics is essential in this case; specialists can look at information, track down the source of the deepfake, or get records from platforms. Sections 65A and 65B of the Evidence Act in India acknowledge electronic evidence. Police are required to maintain chain-of-custody. But as one article points out, it can be difficult to verify deepfake evidence in court; judges now frequently doubt the legitimacy of images in the "era of deepfakes." The onus is on the prosecution to demonstrate that the material is authentic; victims may also have to provide evidence of the defendant's involvement.

B. Injunctive and Civil Remedies

- **Defamation Suits:** If a deepfake causes injury to a victim's reputation, they may bring a civil defamation claim. Since truth is the standard defense, the plaintiff needs simply demonstrate that defamatory content was published. In other situations, plaintiffs have obtained defamatory injunctions against online impersonators, but deepfakes complicate matters because "publication" may occur through anonymous social media.
- **Injunctions by Passing-Off/Trademark:** Public personalities may use unfair competition or passing-off legislation, as was the case in the Warikoo and Kapoor instances. Trademark law may prevent the deepfake if it makes use of a registered trademark (such as "Warikoo") or suggests official support. Even against unnamed defendants, courts have the authority to grant John Doe injunctions, directing platforms to take down or deactivate the content.
- **Copyright:** A victim may allege infringement by unlawful derivative creation if they own the copyright to some of the content (such as an original photo or video utilized in the deepfake). The right to privacy There is no distinct remedy outside of the aforementioned channels, although Article 21 jurisprudence may

bolster claims against excessive deepfake misuse of personal likeness, even though it is not codified.

- **Data Protection Complaints:** If victims' personal information was handled illegally to produce a deepfake, they may also file a complaint with the Data Protection Board under the DPDP Act. (This is a brand-new field with no established predecessors).

Every remedy has its challenges. The anonymity of deepfake makers, who are frequently located abroad, makes prosecution challenging, and criminal cases can be slow. Generic "John Doe" pleadings may be used in civil proceedings against unidentified persons. However, if the court determines a prima facie right, injunctions can be issued quickly. For instance, in past celebrity instances, the Delhi High Court has mandated that social media sites remove Warikoo's deepfake content within 36 hours.

Digital evidence protocols are essential in every situation. When presented in court, electronic recordings (such as video files) must be certified in accordance with Section 65B of the Indian Evidence Act (as amended). Police may need to work with social media firms to collect originals and IP logs, so victims must make sure copies of the deepfake and metadata are kept safe. Courts are aware of the problems with deepfakes; in Nirmaan Malhotra v. Tushita Kaul (2023), the Delhi High Court warned that photographic evidence had to be carefully established and stated that "we are living in the era of deepfakes." This implies that courts will carefully examine any digital evidence for indications of manipulation, which can enable defendants to raise doubts by introducing expert testimony on AI development.

C. Gaps in Law and Enforcement

Even while current legislation addresses several areas of deepfake usage, there are still a number of important gaps

For instance:

- **No Deepfake-Specific Offence:** There is no legislation in India that specifically defines or makes deepfakes illegal. Because of this, authorities are forced to use antiquated clauses (such as impersonation and forgery), which leads to ambiguity, especially when it comes to non-consensual sexual deepfakes. On the other hand, certain U.S. states and the European Union are pursuing mandated disclosures and clear definitions.
- **Anonymity & Jurisdiction Issues:** As demonstrated in the Nirmala Sitharaman case, which involved a suspect residing in the United States, deepfake criminals frequently act anonymously and from overseas, making identification and prosecution challenging because of jurisdictional constraints.
- **Consent & Gender Harms**: While real-image offenses are covered by current legislation (such as BNS Section 77), artificial intelligence-generated sexual imagery might not be. This creates legal ambiguity surrounding permission in synthetic media and forces victims—mostly women—to rely on indirect remedies like defamation or harassment laws.
- **Fake news and political deepfakes:** The laws controlling election-related disinformation are out of date. Additionally, the Representation of People Acts do not include restrictions for synthetic audio-visual misrepresentation, and deepfakes circumvent existing sections on "rumour" or misleading statements. Existing strategies, such as ECI alerts, are insufficient.
- **Evidentiary Gap**s: Strict digital evidence requirements, such as Section 65B certificates, are mandated by Indian courts. Deepfakes take advantage of this by raising questions about authenticity; as a result, courts must now evaluate both the authenticity and artificiality of content.
- **Intermediary Gaps:** Deepfake removal is frequently postponed by platforms. Despite the IT Rules' requirement for takedown within 36 hours, AI detection is still in its infancy and enforcement is uneven.

- **Limited Awareness & Capacity:** Law enforcement is not equipped with the necessary training or resources to recognize phony media. Unless there are high-profile instances, underreporting and investigative failures result from cybercrime units and courts still adjusting.

IX. SUGGESTIONS & WORLDWIDE MODELS

- **Make Particular Offenses:** By changing BNS (e.g., Section 77) and the Representation of People Act, specific measures for deepfakes—particularly non-consensual sexual material and political manipulation—can be introduced.
- **Revise the Intermediary Rules:** Require the labeling of AI-generated content, emulating the EU AI Act. Shorten takedown periods and penalize repeat infractions. To improve AI literacy, start public awareness campaigns, use fact-checking networks to spot deepfakes, and teach people how to spot fake material.
- **Develop Technical Capacity:** To identify deepfake artifacts, educate cyber investigators and purchase forensic equipment. To chase down transnational criminals, promote international collaboration.
- **Enhance Victim Remedies:** Provide access to preserved copies of synthetic media for evidence, expedited civil remedy, and court-ordered takedowns. Make clear that deepfake porn is considered sexual harassment under the law.
- **Control AI Development:** Promote transparency and watermarking in generative AI technologies. Provide developers with responsibility and ethical standards.
- **Periodic Legal Review:** Add references to "AI-synthesized" or "computer-generated" information to the BNS, DPDP, and IT Act. Lawmakers ought to enact more comprehensive offenses that target misleading digital media.
- **Take Note of Global Trends:** Nations such as the United States, Australia, and the United Kingdom are passing legislation that is particular to deepfakes. India

must respect freedom of expression for satirical or creative deepfakes while adhering to international standards.

X. CONCLUSION

The use of deepfake technology puts Indian law to the test. A network of offenses spanning the BNS/IPC, IT Act, privacy standards, and election laws can be applied to different deepfake abuses, even if no specific act was created for it. With its revised definitions of forgery, false evidence, and sexual privacy, the Bharatiya Nyaya Sanhita, 2023, updates Indian criminal law for the digital era. The IT Act offers several ways to pursue deepfake crimes in addition to its rules on identity theft, privacy violations, and pornographic electronic content. These methods have been used in recent court and enforcement actions, such as FIRs against bogus political films and injunctions for AI-generated pornography.

The lack of a specific "deepfake" violation, the anonymity of offenders, cross-border material hosting, and evidentiary uncertainty are some of the major gaps and difficulties that still exist. Victims still have to deal with difficult criminal and civil procedures. India should think about specific changes to address these, such as obligatory labeling for synthetic media, increased intermediary obligations, and explicit deepfake rules (particularly for sexual and political misuse). International experience demonstrates that public education and technical countermeasures are just as important as legal ones.

In conclusion, the Indian legal system has to be improved and adjusted even if it has numerous tools to fight deepfakes. The BNS and IT Act can cover a lot of area, but we encourage stakeholders and legislators to plan ahead because our laws need to change as AI advances. India can prevent malevolent deepfakes and safeguard people's rights and democracy against this new danger by enacting and enforcing laws that are cautious and grounded on evidence.

XI. REFERENCES

- *Bharatiya Nyaya Sanhita, 2023*, Act No. 45 of 2023 (India) (enacted Dec. 25, 2023)

- *The Information Technology Act, 2000*, Act No. 21 of 2000 (India)
- *The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021* (India)
- *Indian Penal Code*, Act No. 45 of 1860 (India)
- *Representation of the People Act, 1950* (India)
- *Representation of the People Act, 1951* (India)
- *Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1 (India)
- *Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors.*, (2017) 10 S.C.C. 1 (India).
- Press Release, Ministry of Electronics & Information Technology, Government of India, "*Government of India Taking Measures To Tackle Deepfakes*" (Apr. 4, 2025)
- Election Commission of India, Press Note No. ECI/PN/72/2024 (May 6, 2024)
- Shinu Vig, *Regulating Deepfakes: An Indian Perspective*, 17 J. Strategic Sec. 70 (2024)
- Swanand Bhale, *Deepfake Laws in India: The Need for Legal Regulation in the AI Era* (unpublished manuscript, Feb. 1, 2025), SSRN
- Parthsarathi Jha *et al.*, *Navigating AI Regulation in India: Unpacking the MeitY Advisory on AI in a Global Context*, ELP Law (Mar. 19, 2024)
- Rishika Priyadarshini & Chitheer Bala, *Legal Dimensions of Deepfake Technology: Privacy, Consent, and Criminal Liability*, Juris Centre (July 27, 2025)
- *The Dilemma of Deepfakes: Expanding the Ambit of Right to Personality to Regulate Deepfakes in India*, Law Sch. Pol'y Rev. (May 4, 2024)