AN ANALYSIS OF THE LEGAL FRAMEWORK GOVERNING DEEPFAKE TECHNOLOGY AND FAKE NEWS PROPAGATION IN INDIA

Submitted by Misthi Saha, Assistant Professor of Law, Sister Nivedita University, Kolkata

Arunabh Biswas, LL.M., Sister Nivedita University, Kolkata

ABSTRACT

Deepfake technology has rapidly emerged as a disruptive force in India, intersecting with fake news propagation to challenge legal, social, and democratic structures. This paper critically examines the adequacy of India's existing legal framework in addressing harms caused by synthetic media, focusing on the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Bharatiya Nagarik Suraksha Sanhita, 2023, the Digital Personal Data Protection Act, 2023, and the Intermediary Guidelines Amendment Rules, 2025–26. While these statutes provide partial safeguards against identity theft, sexual exploitation, fraud, and reputational damage, they were not designed to regulate AI-generated content, leaving significant gaps in enforcement. The IT Act criminalizes impersonation, fraud, and obscene content dissemination, but courts struggle to classify fabricated explicit media as "obscene" or "sexually explicit." The BNS extends traditional offences such as defamation, personation, and criminal intimidation to deepfake contexts, yet evidentiary challenges under the Bharatiya Sakshya Adhiniyam hinder prosecution. The DPDP Act introduces data protection principles, recognizing biometric identifiers as sensitive personal data, but enforcement remains complex when consent overlaps with public sharing. Recent intermediary rules mandate rapid takedown, labeling, and traceability of synthetic content, reflecting a shift toward proactive moderation, though concerns persist about over-blocking and free speech. Comparative insights from the EU's AI Act and U.S. state-level statutes highlight India's evolving but fragmented approach. Ultimately, the study underscores the urgent need for coherent, technologically informed regulation that balances protection of dignity, autonomy, and public order with constitutional freedoms in the age of deepfakes.

Keywords: Deepfake, Deepfake Technology, Synthetic Media, Fake News Propagation, Deepfake legislations.

Introduction

Deepfake technology is being used in fraud, spreading fake news, sexual exploitation, political manipulation, and defamation. Indian Law has had to cope with these problems with few resources and weak regulations.[1] AI technology that can easily put a public figure's voice or face onto a fake news clip is being used to make deepfake videos that look real and are used to commit many crimes across the country[2]. The current laws are not doing enough to stop this, which raises questions about our criminal justice system. This paper begins with the convergence of deepfakes and the spread of fake news. It then looks at the Bharatiya Nyaya Sanhita, 2023 (BNS), the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS), the Information Technology Act, 2000 (IT Act) and its amendments, to see how they create a legal space for deepfake-related crime and victimization. None of these tools were made to deal with deepfake and AI-related crimes like spreading false information.[3] The paper examines the adequacy of the current legal system in addressing these issues and safeguarding dignity, autonomy, and democratic processes in an era where identity can be easily constructed.

The BNS supersedes the Indian Penal Code of 1860; its stipulations regarding defamation, voyeurism, criminal intimidation, and impersonation are now construed to encompass synthetic recordings that misattribute statements or actions, or that threaten the distribution of fabricated intimate content for extortion purposes. The BNSS, which replaces the Code of Criminal Procedure, 1973, does not create any new deepfake crimes. Instead, it changes the way investigations are done by requiring forensic investigations for serious crimes, allowing electronic evidence, and setting rules for searching and seizing digital devices. The Information Technology Act, 2000 (IT Act) and its changing provisions are still the basic law for computer crimes. Laws against identity theft, cheating by pretending to be someone else online, and sending or publishing obscene or sexually explicit content in electronic form have been utilized to go after non-consensual intimate deepfakes.[4] As fake news deepfakes become more common, the same rules are being used to cover AI-generated political films, fake press conferences, and fake "news" pieces that spread quickly on social media and encrypted messaging apps.

[1] Sommya Kashyap, The Digital Mirage: India's Evolving Legal Battle Against Deepfake Technology, SCRIPTed, Vol 22, Issue 2
[2] Ibid
[3] Ibid
[4] Information Technology Act, 2000, ss 66, 66C, 66D, 67, 67A

Research on recent elections and the COVID-19 pandemic indicates that AI-generated text and video are frequently employed to construct deceptive yet persuasive news ecosystems, wherein articles, photos, and deepfake videos mutually reinforce each other while taking advantage of platform algorithms that prioritize user interaction.[5] Deepfakes aimed at public officials, medical professionals, or journalists undermine trust in both individual speakers and the epistemic authority of "news" in general. This creates what some authors call "reality apathy," a state in which people can't tell the difference between real and fake content[6]. This is also starting to happen in India, where stories of fake clips in many Indian languages being used as proof of communal crimes, corruption, or election fraud and then being denied as fake are starting to come out.[7]

A study on image-based sexual abuse and cyber-enabled gender violence illustrates how intimate deepfakes integrate into a broader spectrum of harms, encompassing voyeurism, "revenge porn," sextortion, and the non-consensual dissemination of personal photos.[8] These abuses often cross over into the fake news business, where intimate synthetic photographs and videos are uploaded to porn sites, reposted on social media with fake news titles, and occasionally covered by bad news outlets as "celebrity leaks" or "viral MMS scandals."[9] In these situations, deepfakes serve as tools for gender-based abuse while also being highly engaging "news content" in a platform economy that makes money from clicks and shares.[10]

Legal framework in India Regarding Deepfake Technology

India has laws that address the use of "deepfakes" through existing legislation, such as the Information Technology Act 2000, the Bharatiya Nyaya Sanhita 2023, and the Digital Personal Data Protection Act 2023. Therefore, these laws should provide some level of protection from identity theft, image-based sexual exploitation, fraud or deception from the use of deepfakes and fake news.[11] However, since these laws were written to apply to the transmission of digital

[5] Nasiri & Hashemzadeh, The Evolution of Disinformation from Fake News Propaganda to AI-Driven Narratives as Deepfake (2025) 9 J
[6] Ibid
[7] Election-period reporting on political deepfakes and communal content in India.
[8] Kabra & Gupta, 'Carving an Indian Mosaic for Image-Based Sexual Abuse' (2022) 34 Natl L Sch India Rev 205,
[9] Ibid
[10] Ibid
[11] Sommya Kashyap, The Digital Mirage: India's Evolving Legal Battle Against Deepfake Technology (2025) SCRIPTed 162, 163–64.

content rather than its creation, they do not fully protect individuals from being victimized by the use of deepfakes.[12]

1. Information Technology Act 2000

The IT Act continues to be the most applicable law when someone commits a deepfake offence using "computer resource" or "communication device." Section 66C renders it an offence to counterfeit or otherwise improperly use another person's "electronic signature, password or other unique identifier" in a deepfake context; therefore, the making of synthetic images or sounds, such as through a "digital arrest" scam or a fake emergency fund transfer call, would fall under that section's provisions. A person found guilty under Section 66C could be sentenced to three years' imprisonment or fine.[13] Courts interpret provisions broadly enough to include the use of AI to impersonate someone by using their voice or face to get into systems or make a false story more believable, such fake news videos that are part of phishing schemes. Cheating by impersonating another person using a computer or other communication device has been an element of Fraud, Section 66D; consequently, section 66D has been cited in deepfake calls/videos that have purported to be made from, or to be the result of, an agency such as the police department, customs other tax authorities, or through a business entity (executive). These deceptions have accomplished their objectives through the conviction of the victim to send money as well as to acquire private information.[14]

Sections 67 and 67A talk about sending or publishing obscene and sexually explicit information electronically. These laws have already been utilized against those who shared sexual content or posted AI-morphed private pictures, frequently disguised as shocking "news" about actors or regular women.[15] The challenge arises because the sections were established prior to the advent of deepfakes, necessitating judicial determination of whether a fabricated explicit video generated by deepfake qualifies as "obscene" or "sexually explicit" in the same manner as a genuine recording, and whether the absence of the underlying act mitigates harm.[16] Research articles on image-based sexual abuse contend that the dignitary, psychological, and reputational

[12] Ibid
[13] Information Technology Act 2000, s 66C.
[14] Information Technology Act 2000, s 66D.
[15] Aanchal Kabra & Rohit Gupta, 'Carving an Indian Mosaic for Image-Based Sexual Abuse' (2022) 34 Natl L Sch India Rev 205, 212–13
[16] Kashyap (n 1) 172–73

harms of deepfake pornography are comparably significant, and at times more severe, than those associated with traditional non-consensual imaging.[17]

Section 69A gives the government the ability to prevent public access to material "generated, transmitted, received, stored, or hosted in any computer resource" for reasons including sovereignty, public order, or incitement to an offense.[18] In practice, it has been used to inform intermediaries to take down or block URLs and accounts that share deepfake content, such as politically controversial or community fake news videos.[19] The blocking power is officially content-neutral, but in the case of deepfakes, it lets the government quickly respond to AI-generated fake news that could hurt the integrity of elections or the peace of the community. For example, a fake speech that incites violence or a fake "sting" of a candidate accepting bribes.[20]

Intermediaries must comply with Section 79 and the 2021 Intermediary Guidelines and Digital Media Ethics Code Rules to be protected from platform liability. Intermediaries that have fulfilled their due diligence requirements such as appointing grievance officers, removing flagged content within the expected time, and using automated tools to identify certain forms of harmful content will be considered to have a safe harbour for third party user-generated content.[21] The draft amendments proposed in 2025 for the first time included a definition of "synthetically generated information," as well as duty obligations for a large platform to collect user declarations, verify automatically as well as to label synthetic content and trigger where content appears "reasonably to be authentic or true."[22] The surge in deepfake and false news incidents, including viral video campaigns of political figures and fake celebrity news “leaks”, [23]has been an explicit justification for developing policy solutions and/or looking for new ways to address these events. However, many critics have raised concerns that current and proposed detection tools will have difficulty distinguishing between lawful, parody, and acceptable generative uses from some forms of harmful deepfake content, and that the use of false positive

[17] Kabra & Gupta (n 8) 205–17, 234–38
[18] Information Technology Act 2000, s 69A and Rules.
[19] Ministry of Electronics and Information Technology, Advisory on Deepfakes (Nov 2023).
[20] Election Commission of India, Guidelines for Synthetic Media in Elections (Jan 2024)
[21] IT Intermediary Guidelines and Digital Media Ethics Code Rules 2021, rr 3–4.
[22] Draft IT (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules 2025, proposed r 2(1)(wa), r 3(1)(x)–(z).
[23] MeitY press and policy commentary on deepfake regulation.

detection could negatively impact free speech on the political spectrum.[24]

2. Bharatiya Nyaya Sanhita 2023

The BNS 2023 provision is an alternative to the Indian Old Penal Code and it/They directly supply the substantive offences that are now used to charge deepfake conduct once the "computer resource" element brings the IT Act into play.[25] A dedicated deepfake criminal activity was not included in the plan however there are numerous sections that are related when disinformation is portrayed by synthetic media or to do harm to objects.

Cheating by personation, which is defined under section 319, refers to deceiving any person "by pretending to be some other person" or by knowingly substituting one person for another.[26]Deepfake impersonations-like a video of a politician announcing a fake policy, for example, or an audio clip of a bank officer instructing a fund transfer-are the quintessential notion of personation, but they function mostly through availability to the masses rather than being operated on the basis of individual communication.[27] This generates issues of interpretation, whether the crime presupposes that every deceived viewer has to interact with the person directly or if "news clips" of deepfakes, which are directed to an undifferentiated audience, would be sufficient.[28]

Section 356 on defamation is the most direct criminal path to take for the reputational damages where deepfakes attribute false statements or conduct to a person[29]. A hypothetical video designed to look like a judge accepting a bribe or a community leader performing a hate speech that never took place, can indeed prove the elements of imputing something that harms the reputation.[30] The key issue, however, is the question of evidence: proving that a hyper-realistic video is synthetic, and that the accused either knew or should have known it was false when causing its publication.[31]

The criminal use of deepfakes as a method of coercion to obtain money or to drop complaints

[24] Ashima Obhan & Arnav Joshi, 'Fine-tuning India's Draft Rules on AI Synthetic Media' (2025).
[25] Bharatiya Nyaya Sanhita 2023, Preamble.
[26] Bharatiya Nyaya Sanhita 2023, s 319.
[27] Vakul Sharma, Information Technology Law and Practice (4th edn, 2023) 234.
[28] Kashyap 177–78.
[29] Bharatiya Nyaya Sanhita 2023, s 356.
[30] Ibid
[31] Ibid

is covered under section 351 Criminal Intimidation.[32] The potential harm does not arise solely from the ultimate act of publishing; however, it arises also from the fear that a viral explosion of fake news could occur using the fictitious materials in question at some time. The courts have also considered section 77, Voyeurism and Image-Based Sexual Abuse to be applicable to the production and distribution of non-consentual deep-fake pornographic images[33]. Although, this statute was intended to apply to conventional photos and videos. The court will ultimately determine whether creating a composite of an individual's face on an already created explicit video constitutes "capture" or "transmission" of an image of private body parts, as well as, what legal consequences may result from the distribution of such content with sensationalized captions in a format resembling fake news.[34]

BNS provisions concerning "public nuisance", "promoting enmity" and other criminal offenses may be applicable as well regarding fake-news deep fakes which endanger public order, especially if synthetic video is employed to incite violence among different communities and/or to fraudulently lead voters to make erroneous decisions about candidates or government officials.[35] In addition, an example of political deep fakes from the 2024 Indian general election artificially created images of political leaders and/or animated by artificial intelligence to represent state chief ministers, demonstrates how the use of digital media can be combined with organized misinformation campaigns instead of just random pranks.[36] In such cases, prosecutors tend to rely on a combination of BNS public-order offences and IT-Act computer crimes, with BNSS providing the procedural tools for electronic evidence and forensic analysis.[37]

3. Digital Personal Data Protection Act 2023

Whereas both the IT act and the BNS legislation address "content" and "conduct," the DPDP Act 2023 focuses on the flow of data through which deepfake technology is made possible. The Act also defines "personal data" in a broad manner to include all information related to an identifiable individual; it specifically identifies biometric identifiers (such as facial images or voice prints) as being "sensitive personal data," therefore entitled to additional protections.[38]

[32] Bharatiya Nyaya Sanhita 2023, s 351
[33] Bharatiya Nyaya Sanhita 2023, s 77.
[34] Vakul Sharma, Information Technology Law and Practice (4th edn, 2023) 245.
[35] Kashyap 168–69, 196–98
[36] Nilesh Christopher, 'AI and Deepfakes Played a Big Role in India's Elections' (2024).
[37] Bharatiya Nagarik Suraksha Sanhita 2023; I4C Annual Report 2023–24.
[38] Digital Personal Data Protection Act 2023, ss 2, 6–7, 33(6

Free, Specific, Informed, Unconditional, Unambiguous consent is required for data processing in order to process personal information on behalf of others. The purpose of which must be clearly defined. Personal Data Processing beyond this defined purpose without a valid reason may result in regulatory actions.[39]

The same individuals who are creating deepfakes with the aid of artificial intelligence (AI) and machine learning (ML), or those who use these tools to create malicious content, are using your facial features and voice by scraping them off social media platforms such as Facebook, Instagram, LinkedIn, etc., YouTube videos, interviews and leaked databases to train their AI/ML models, so they can generate your fake identity.[40] Harvesting and storing such scraped materials without obtaining appropriate consent, and/or failing to protect the scraped materials with sufficient security measures would be breaches of the obligation of purpose limitation, obligation of data minimization, and obligation of reasonable security measures under the Data Protection Principles of Purpose Limitation, Data Minimization, Reasonable Security Practices, etc., of DPDP Act, if the scraped material has been harvested by a data fiduciary having its place of business in India. [41]Further, some scholars suggest that regulators could take action against both those who carried out the high-impact incident (e.g. a deep-fake campaign based upon leaked biometric information), if they can be identified, and also against any data fiduciaries whose negligence led to the misuse[42]

Deepfakes are created when content creators/malicious individuals collect images of people's faces and/or recordings of their voice through scraping social media platforms, news/entertainment programs or other sources including leaked databases.[43] If the person collecting the content is a data fiduciary based in India and collects this information without the individual's consent or stores it improperly, they would likely be violating at least three requirements of the Data Protection (DPDP) Act: limiting how the data can be used for its stated purposes; minimizing the amount of personal data collected; and implementing proper security measures.[44] In cases involving major impacts such as large-scale misinformation or propaganda campaigns based upon stolen facial recognition data authorities may choose to

[39] Ibid s 6–7, 11–12
[40] Priya Menon, 'The Deepfake Conundrum: Can the DPDP Act, 2023 Deal with Misuse of Generative AI?' (2023) IJLT (online).
[41] Ibid
[42] LHSS Collective, 'Deepfakes and the DPDP Act' (2024)
[43] Priya Menon, 'The Deepfake Conundrum: Can the DPDP Act, 2023 Deal with Misuse of Generative AI?' (2023) IJLT (online)
[44] Ibid

prosecute both those who use the stolen data to create and disseminate misinformation/deepfakes, if they can identify them, and those who failed to protect the stolen data.[45]

The Act provides data subjects with several rights; namely, access, correction, deletion (or "right to be forgotten") and grievance resolution.[46] In practice, if someone is the victim of a deep fake video or photo they may make an application under the right to delete against the platform or intermediary who hosted this data on behalf of the data subject, claiming it includes their personal information that has been illegally processed or processed outside of the original processing context.[47] However, there will likely be two major obstacles. Firstly, most deep fakes are created using media originally published by the data subject themselves for some other use. This raises problems regarding how far back the scope of consent can reasonably extend when the content has been made public.[48] Secondly, DPDP provisions sit beside and will need to be weighed against the requirements of Freedom of Expression as well as Journalistic/Research Use, making removal applications difficult when the synthetic content is included in news reporting or political commentary.[49] The DPDP Act does not directly control what is true or false with respect to the content that is provided in a post or article; however, the DPDP Act has the potential to restrict the supply of biometric information from which the fake news video or image (deepfake) is created and provide incentives for social media companies and other large data fiduciaries to implement safeguards to protect their systems against unauthorized access through scraping and breach.[50] However, while this type of regulation may also have a negative impact upon legitimate archival, reporting and training purposes, there is likely to be an ongoing challenge for regulators as they attempt to issue guidelines that are both specific enough to be useful and general enough to be enforceable.[51]

4. Intermediary Amendment Rules 2025

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules of 2025 is the first time India has attempted to include "Synthetic

[45] LHSS Collective, 'Deepfakes and the DPDP Act' (2024).
[46] Digital Personal Data Protection Act 2023, s 11–12
[47] Ibid.
[48] Menon (n 34)
[49] Puttaswamy v Union of India (2017) 10 SCC 1.
[50] Nasiri & Hashemzadeh, 'The Evolution of Disinformation from Fake News Propaganda to AI-Driven Narratives as Deepfake' (2025) 9 J Cyberspace Stud 229, 233–39.
[51] LHSS Collective (n 36)

Genetically Generated Content" in its intermediary liability law.[52] The 2025 Notification will add a definition of "intermediary due diligence" to include a requirement for intermediaries to remove content which is either illegal as traditionally defined or created with the use of artificial intelligence such as deepfake technology intended to threaten the sovereignty, national security, public order, morality, health, decency or defamation and incitement.[53] This 36 hour notice period will now be used to provide an opportunity for a potential "deep fake" video to go viral and potentially have an impact on an election or exacerbate a communal issue while it takes at least 36 hours for a normal investigation to begin.[54]

User statements regarding whether or not a user-generated item of Content has been created by an AI would need to be collected by large Social Media Intermediaries. In addition, the intermediaries would need to verify those User Statements using "Reasonable Technical Measures." Finally, Social Media Intermediaries would need to add visible labels and metadata to all items of Content that appear to be Synthetic.[55] Those same intermediaries would also be expected to use automated tools to identify and flag categories of Prohibited Synthetic Content (e.g., Deep Fake Pornography, Forged Documents, Fabricated News Clips). However, even though they may use these Automated Tools to detect categories of Prohibited Synthetic Content, Social Media Intermediaries will still enjoy Safe Harbor protection if they operate in good faith pursuant to Section 79 of the Information Technology Act.[56]

As well as providing definitions, the 2025 amendment rules also introduce more timely removals.[57] Specifically, it has defined "deepfakes" and reduced the timeframes for removal.[58]The definition states that deep fakes are audio-visual content which changes a persons' identity, voice or behavior via an artificial intelligence tool that could lead to the deception of viewers. It does however exclude normal video editing and accessibility features.[59] An intermediary will have to remove or block flagged "deep fake" or other harmful synthetic content within 3 hours after receiving a notice of infringement from a user, a third party (such as a 'trusted flagger'), or from a government order. In addition to the above

[52] IT (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2025 (India).
[53] Id
[54] IT Rules 2021 r. 3(1)(d), as amended in 2025.
[55] CyberPeace Foundation, Outlook on the 2025 Amendments to the IT Intermediary Guidelines.
[56] "Decoding the Proposed IT Amendment Rules, 2025," The Leaflet (Oct. 23, 2025).
[57] IT (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, G.S.R. 120(E), 10 Feb. 2026.
[58] Aayushman Gaikwad & Smruti Mishra, "India's New Rules For AI-Generated Content And Deepfakes," LiveLaw (Feb. 21, 2026).
[59] Ibid

obligations, significant social media intermediaries are required to provide metadata so that their users can be traced back to the original source. They will be required to retain logs of all activities related to the generation and dissemination of this content and establish separate complaint resolution mechanisms for harm caused by AI-generated content. If either obligation is breached there is a risk of losing safe harbor.[60] Legal commentators note that these rules represent a move from reactive moderation to proactive measures, focusing on speed and technological traceability; however, there remains some concern regarding potential over-blocking, and how smaller platforms can develop sophisticated detection technology.[61]

5. Bharatiya Nagrik Suraksha Sanhita AND Bharatiya Sakshya Adhiniyam

The Bharatiya Nagarik Suraksha Sanhita 2023, in addition to the Bharatiya Sakshya Adhiniyam 2023, will help bring Criminal Procedure and Evidence Law into the Digital Era. [62]The BNSS's Provisions on Investigation, Search and Seizure of Electronic Devices as well as Production of Electronic Records are intended to improve how Police and Courts deal with Digital Evidence (e.g. alleged Deep Fakes).[63] The Bharatiya Sakshya Adhiniyam replaces sections 65A and 65B of the Indian Evidence Act with a more detailed framework for admissibility and proof of electronic records, including authenticity requirements.[64]

Study showed that cybercrime units usually do not have specialized forensic equipment and education necessary to determine whether an item of audio-visual content is real, or has been altered by manipulation; that there is limited expertise in the area of recognizing synthetic material in most of the country, and that this expertise is concentrated in a small number of metro labs.[65] In addition, scholarly studies of deep-fake evidence under BSA 2023 warn that while the new law updates terminology, it does not provide concrete standards or protocols for verifying synthetic media, so courts will rely almost exclusively on disputed expert testimony to verify the authenticity of deep-fake video or audio.[66] Therefore, many deep-fake driven fake

[60] Nishith Desai Associates, "AI-Generated Content and Combating Deepfakes: What India's New Rules Mean for Global Platforms" (Feb. 18, 2026).
[61] Dalmia, "Regulation of AI-Generated/Deepfake Content & Synthetically Generated Information," LinkedIn article (Feb. 12, 2026)
[62] Bharatiya Nagarik Suraksha Sanhita, 2023; Bharatiya Sakshya Adhiniyam, 2023
[63] Ministry of Home Affairs, BNSS Overview Notes (2024).
[64] Pinky Bansal, Future Challenges of Electronic Evidence: Deepfakes, AI Data, and Blockchain under BSA 2023 (2024)
[65] Kashyap, supra note 1, at 203–05, 216–19
[66] Bansal, supra note 26; "Deepfake Evidence and Criminal Trials: Challenges to Justice in the AI Era," J. Legal Res. & Polity 1(1) (2025).

news cases either fail because they cannot meet evidentiary requirements, or are never submitted for prosecution as complete criminal trials, which reduces the effectiveness of the deterrent provision of the BNSS and provisions of the Information Technology Act (IT Act)[67]. Timing is critical when dealing with propaganda through fake news. By the time a deep-fake is analyzed using forensic techniques and verified to be non-authentic via BSA compliant processes, the election cycle or community event it was intended to target may have already ended.[68].Although BNSS allows for quick filing of e-FIRs and electronic complaint registrations, without corresponding investments in detection and forensic capabilities, the above referenced modernization of procedure does not currently represent effective control over synthetic disinformation.[69]

Global Legal Framework

1. European Union: AI Act and Platform Duties

The European Union's artificial intelligence legislation to date (the Artificial Intelligence Act) 2024 takes the most complete legislative approach by using a classification system based on risk categories for "transparency" problems rather than creating a new offense for "deep fakes".[70] When providers of artificial intelligence (AI) systems create or alter images, audio or video they must clearly identify it as created artificially.[71] Deep fake content will have to carry labels that allow ordinary viewers to understand what they are viewing. In addition, the European Unions' Digital Services Act and General Data Protection Regulations (GDPR), require platforms to host, remove quickly (in relation to deepfake news content), conduct risk assessments and comply with data protection regulations when hosting deepfake news content.[72]

2. United States: State-Level Criminalisation

There is no single, federal deepfake statute in the U.S., however many states are taking on specific harms; for example, non-consensual pornography and electoral manipulation.

[67] Kashyap, supra note 1, at 210–11.
[68] Id. at 204–05.
[69] Indian Cyber Crime Coordination Centre, Annual Report 2023–24, 67–80 (2024).
[70] Analytical Study of the World's First EU Artificial Intelligence (AI) Act, Int'l J. Res. & Publication Rev. (2024).
[71] Regulation (EU) 2024/… Artificial Intelligence Act, arts. 50, 52 (transparency and deepfake disclosure obligations).
[72] EU GDPR arts. 5–9; Digital Services Act 2022.

California has created a civil cause of action for an individual who has been shown in sexually explicit deepfakes without their consent. Additionally, California prohibits the distribution of material deception and/or unlabeled audio-visual media of candidates in an election.[73] Non-consensual pornography and election laws in Virginia and Texas were both amended to include morphed or AI-generated videos of an individual engaging in an intimate act(s) or misleading campaign clips, if sufficient evidence exists to prove the intent to deceive voters or violate a reasonable expectation of privacy.[74] The above state statutes are in addition to other torts including defamation and intentional infliction of emotional distress. Many U.S. legal scholars believe that these torts still create significant gaps for satirical or "labelled" deepfakes that may be harmful but also protected by constitutional law. [75]

3. China and East Asia: Licensing and Watermarking

China chose a "command-and-control" approach by implementing regulations of "deep synthesis," (generative) AI including name registration for suppliers, technical security evaluation of their services and implementation of watermarks in synthetic video-audio.[76] In addition, deep synthesis providers are required to identify synthesized media and guarantee that generated content will not violate national security laws nor cause disturbances in economic or social orders nor infringe upon individuals' right to privacy.[77] Similar issues in South Korea and Japan focus on image-based sexual abuse and impersonations of celebrities; each country is proposing amendments to their sexual-violence and/or personality-right legislation to protect citizens from use of AI-generated pornography, and/or avatar-harassment.[78]

4. UNESCO Recommendation on the Ethics of Artificial Intelligence (2021)

While there are no global "deepfake" conventions currently being drafted by the U.N., an accumulation of several agreements collectively provide a weak foundation upon which deepfake-driven fake news could be regulated. One of the primary agreements is UNESCO's

[73] Matthew B. Kugler & Carly Pace, Deepfake Privacy Attitudes and Regulation, 116 Nw. U. L. Rev. 611 (2021).
[74] Cal. Civ. Code § 1708.86; Cal. Elec. Code § 20010.
[75] Va. Code Ann. § 18.2-386.2; Tex. Penal Code § 21.16; Tex. Elec. Code § 255.004.
[76] Provisions on the Administration of Deep Synthesis Internet Information Services (China 2022).
[77] Id
[78] Comparative overview in Jayashree J. et al., Deepfake Cyber Threats in India: An Emerging Challenge Without Legal and Technical Safeguards, IJERT Vol. 14, Issue 1, at 3–4 (2024).

2021 Recommendation on the Ethics of Artificial Intelligence (the "Recommendation"), which was ratified by UNESCO's General Conference; this agreement considers AI-generated, and algorithmically amplified content as part of a larger problem of disinformation and hate speech not as a standalone technical problem.[79] The Recommendation requires member states to make investments in digital, media and information literacy programs, to support users' ability to recognize the impact of AI systems on what they view, and to assist them in their critical analysis of synthesized or manipulated content rather than simply trusting it.[80] As referenced within the paper, this recommendation provides additional support for the position stated in the paper that any appropriate Indian response to deep-fake driven misinformation must focus beyond creating criminal prohibitions and/or intermediate regulation requirements and must consider the capability of audiences to identify, and reject, synthetic media. Similarly, the Recommendations further urge states to foster an environment where independent media organizations have rights and resources necessary to report on both the benefits and risks associated with AI systems and to promote the use of AI tools by news organizations in accordance with applicable professional ethics standards.[81] In the context of deepfakes, the Recommendations reinforce your concerns regarding how false videos/audio will not only utilize platform virality to spread, but also put additional strains on already fragile journalism institutions, which require both legal protection and technical capabilities in order to rapidly counter synthetic propaganda.[82]

Parallel work by UN human rights mechanisms adds another layer to this emerging framework. Special Rapporteurs on freedom of expression and related mandates have linked disinformation to attacks on journalists, minorities and elections, and have begun to single out synthetic and AI-generated media as tools that can fabricate compromising material, simulate incitement or confession, and flood public debate with audiovisual “evidence” that is difficult to verify.[83] These reports do not endorse broad “fake news” offences; instead, they call for transparency obligations, narrowly tailored restrictions and effective remedies for victims of online abuse.[84]That approach mirrors the structure of your reform proposal: rather than criminalising fake news in general, the dissertation suggests clearly defined deepfake offences, calibrated

[79] UNESCO, Recommendation on the Ethics of Artificial Intelligence pmbl. (2021).
[80] Ibid
[81] Ibid
[82] See, e.g., U.N. Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Report on Disinformation and Freedom of Expression, U.N. Doc. A/76/258 (2021).
[83] Ibid
[84] Ibid

intermediary duties and deepfake-aware evidentiary standards, all constrained by constitutional guarantees of free expression and privacy. The UNESCO Recommendation also asks States to translate its ethical principles into domestic norms across policy areas including data governance, communication and information, education and justice.[85]

Conclusion.

The current legislative structure of India provides limited legal frameworks for creating and utilizing deepfakes as a means to propagate fake news. Although there are certain laws and regulations that can be "stretched" to apply to the harms caused by deepfakes, the structure of India's legislation on this subject matter is inherently lacking in terms of adequate protections and accountability mechanisms.[86]

There are numerous sections within the IT Act, BNS, etc., that can potentially be utilized to prosecute those responsible for generating, disseminating or otherwise contributing to the spread of deep-fake related fake news. For example, section 66C of the IT Act makes it an offense to steal someone else's identity online while using a computer system or network; section 66D makes it an offense to cheat by personating someone else online via computer system/network; both of these offenses have been utilized successfully in cases involving deepfakes such as scammers making deepfake phone calls, digital arrest scams, impersonators claiming to represent legitimate organizations or officials depicted in fake video clips, and others.[87] Section 67 of the IT Act also addresses obscene and sexually explicit electronic content, therefore prosecutors have been able to utilize this provision with regard to non-consensual deepfake pornography circulating as leaked MMS or scandalous video formatted like real news.[88] Section 69A enables the Government to deny users access to URLs/accounts that host inflammatory/election-related content created via deepfakes that could cause public disorder.[89] The BNS 2023 established substantive offenses for various crimes including cheating by personation (section 319); defamation (section 356); voyeurism/image-based sexual abuse (section 77); criminal intimidation (section 351); and public mischief/security-

[85] UNESCO, supra note 1
[86] Sommya Kashyap, The Digital Mirage: India's Evolving Legal Battle Against Deepfake Technology, 22 SCRIPTed 162, 170–79 (2025).
[87] Information Technology Act, No. 21 of 2000, S. 66C–66D (India)
[88] Information Technology Act S. 67–67A
[89] Information Technology Act S 69A and Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009.

related false information (sections 353 & 195)[90]. Each of these offenses can be pursued in cases where a politician/judge/doctor/community leader was misrepresented in a synthetic clip depicting them stating/demonstrating something they never actually said/did.

Although, the Framework has all weapons available to be effective as an anti-deepfake (or) fake news solution, the academic community describes it as an ineffective tool because it is described as "reactive," "inadequate" and "fragmented." [91]

The first major gapin terms of concept is definitional. In fact, prior to 2026 amendments to the IT-Rules there was no statutory definition of "Deep Fake" or "Synthetically Generated Information," under most of the principal statutes[92]. The definition for Deep Fake News does exist but it is located in delegated legislation for compliance purposes of intermediaries only; therefore, currently, definitions of Deep Fake News do not exist in criminal or evidence law. As a result of this lack of statutory definition courts and police have to fit artificial intelligence-generated pornography leaks, artificial voice-press conference recordings and manipulated newscasts into generic offenses such as fraud, obscenity, defamation or public mischief. These applications create issues with doctrinal certainty with regard to what constitutes forbidden DeepFake News and also make distinguishing manipulative content from satire or legitimate editing difficult; further, it will require each judge to determine policy on a case-by-case basis.[93]

The second major gap in law as it relates to evidence is in the way of proving and process. The BNSS 2023 and the Bharatiya Sakshya Adhiniyam do create new processes for the use of digital evidence and the search of devices; however, both the BNSS 2023 and the Bharatiya Sakshya Adhiniyam remain based upon the assumption that the issue of authenticity is centered around what happens after evidence has been seized (e.g., whether someone has tampered with evidence) and how hash values can determine whether an original file exists. Research and comments discussed within the paper include that there are only a small number of cybercrime labs located in metro areas equipped to detect deepfakes; all other police units lack specialized equipment and training to conduct these types of analyses; and, as such, courts will likely rely

[90] Bharatiya Nyaya Sanhita, 2023, S 77, 195, 319, 351, 353, 356 (India).
[91] Kashyap, supra note 2, at 223–26
[92] Draft Information Technology Intermediary Guidelines and Digital Media Ethics Code (Amendment) Rules, 2025 (India)
[93] Kashyap, supra note 2, at 174–79.

on expert testimony from each side in order to make a determination regarding whether a particular video or audio file is synthetic. Due to this disparity in time (i.e., deepfake fake news can be damaging within hours or days and then often takes months or years to investigate, obtain forensic opinions and reach trial), many deepfake cases either never progress past a preliminary complaint or are dismissed when investigators cannot prove authenticity to the criminal burden. As such, even if laws seem to address deepfake news, they typically fail to provide timely consequences.

The third, platform-based systemic lacuna relates to the amplification of misinformation. The due diligence obligations imposed by section 79 of the IT Act (as amended) and the 2021 intermediary guidelines, as further amended by the 2025 draft amendment rules, and as further clarified by the 2026 draft deep-fake rules require intermediaries to take-down notice of objectionable material upon receiving a complaint; however, the majority of the provisions are content-orientated.[94] To date, there have been very few, if any, legally enforceable obligations placed on intermediaries to adjust or modify the algorithms used to rank and recommend synthetic "news" to users' feed pages.[95] In addition, encrypted messaging has become a major vector for the dissemination of deep fake misinformation in India.

The fourth gap exists in data protection and victim redress. The Data Protection, Privacy and Electronic Communications (Amendment) (EU Exit) Regulations 2019 ('the DPDP Act') could theoretically be utilised against the data fiduciaries who permit the scraping or leak of biometric data to enable the creation of deep fakes and provide a legal entitlement to the data principal to require the removal of their personally identifiable information where this has been illegally processed and displayed within a video of a deep fake[96]. However, in practice, much of the materials used for training are sourced from posts made by users on social media sites for entirely different reasons. Therefore, the extent to which such consent was legally obtained is unclear and so too is whether an illegal process occurred. Furthermore, DPDP Act only addresses itself with regards to the legitimacy of collecting and using the original personal data. It provides no regard to the authenticity/accuracy of the output created as a result of that original

[94] Information Technology Act S79; Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, rr. 3–4; Draft Amendment Rules 2025; draft 2026 deepfake rules.
[95] Indranath Gupta & Lakshmi Srinivasan, Evolving Scope of Intermediary Liability in India, 15 N.U.J.S. L. REV. (2022); Surya S.K. & T.S. Pavan, Regulating Fake News on Social Media Platforms, INT'L RES. J. ADVANCED ENG'G & SCI. (2024).
[96] Priya Menon, The Deepfake Conundrum: Can the DPDP Act, 2023 Deal with Misuse of Generative AI?, INDIAN J. L. TECH. (online 2023).

personal data being inputted into the system. This means that whilst the DPDP Act may be able to limit the sources of highly personalised deep fake propaganda, it does nothing to assist victims of deep fakes with obtaining either swift identification of individual fraudulent/fake news deep fakes as such, removals of those images/videos from all relevant platforms and/or compensation for harm caused as a result.[97] Research both empirically and doctrinally have identified that at present victims have little recourse to address their grievances as they have limited options in terms of filing slow moving criminal complaints, uncertain civil defamation claims and inconsistent platform policies.[98]

[97] LHSS Collective, Deepfakes and the DPDP Act (2024).
[98] Kabra & Gupta, supra note 5, at 205–18; National Cybercrime Reporting Portal statistics, 2019–2024 (deepfake-related tables).