

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS



Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

**Copyright © International Journal for Legal Research & Analysis.
All rights reserved.**

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

DEEPPAKES AND CRIMINAL LIABILITY IN INDIA: A CONSTITUTIONAL AND CRIMINAL LAW ANALYSIS

AUTHORED BY - SIMRAN KUMARI

ABSTRACT

Deepfake technology has quickly raised concerns with regard to criminal law, fundamental rights and regulation in India. While there might be some legitimate purposes for which the technology can be employed, such as artistic purposes, parodies, journalistic reporting, access and entertainment, any abuse of such technology can cause harm with regard to privacy, dignity, reputation, property, public order, and individual autonomy. This paper seeks to explore whether the Indian legal system will have sufficient legal tools to respond to the harms without unduly impinging upon constitutionally protected expression. It will discuss constitutional issues of deepfakes based on that the Article 14, 15, 19(1)(a), 19(2), and 21 on privacy, dignity, reputation, equality and proportionality. We will be looking at the use and restrictions of various legislation such as Bharatiya Nyaya Sanhita, 2023, Information Technology Act, 2000, the Protection of Children from Sexual Offences Act, 2012, Digital Personal Data Protection Act, 2023 and amendments about intermediaries. This research will analyse the differences in legislation on deepfakes in the EU, the USA, and China, and other legislative methods. Any attempts to deceive by creating a fake identity or character will be treated as a crime, with appropriate punishments, ways to prove it, and a process for victim redress.

Keywords: Deepfakes, Criminal Liability, Bharatiya Nyaya Sanhita, 2023 (BNS), Article 21, Article 19, Recommendations.

I. INTRODUCTION

This particular video was uploaded in November 2023 and depicted the face of the actress Rashmika Mandanna placed on the body of some other woman, and it gained wide popularity in India before being discovered to be fake content.¹ Although not the first example of deepfake

¹ Kimika Bhardwaj & Shruti Goyal, *Deepfake Crimes and Criminal Justice: Evaluating India's Legal Response Under the Bharatiya Nyaya Sanhita, 2023*, 2 INT'L J.L. CULTURE & SOC'Y no. 3, at 123, 123 n.1 (July–Sept. 2026) (citing

technology used to produce such impersonation in India and certainly not the worst, the video did manage to move the issue from the technical domain to the public domain. The Union Government issued notices to intermediaries, and by February 2026 the intermediary rules had been rewritten in terms of a new class of controlled content, “synthetically generated information.”² Criminal law legislation has been a slower process, and no provision in the Bharatiya Nyaya Sanhita, 2023 (BNS) addresses the problem of synthetic media; all of the relevant offences are based upon forgeries and impersonations of letters and photographs.³ The problem is made more difficult by the reality that deepfakes themselves are not illegal. The process behind the creation of a deepfake, which creates a pornographic picture of an ordinary citizen, also creates dubbing for movies, helps people with disabilities, and provides political satire.⁴ One single artefact can violate privacy, dignity, reputation, public order, election integrity, and at the same time, be covered by protected speech.⁵ An act of criminal law that does not take into consideration the dual nature of the offence would either not sufficiently protect the victims or reach too far into the territory of Article 19(1)(a) covered speech.⁶

II. DEEPFAKES: TECHNOLOGY AND HARM

"Deepfake" is formed by combining "deep learning" and "fake."⁷ Autoencoders are used in many face swap applications, where the input face is converted to a code representing the facial attributes by an encoder and then reconstructed back by the decoder; exchanging decoders for two different faces results in an image having attributes of one person but with expressions belonging to the other one.⁸ Generative adversarial networks (GANs), proposed in 2014, comprise of a generator that generates the data and a discriminator, which determines whether

Press Release, Ministry of Electronics & Information Technology, Advisory to Intermediaries on Deepfakes and AI-Generated Content (Dec. 26, 2023)).

² Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, G.S.R. 120(E) (India) (notified Feb. 10, 2026; in force Feb. 20, 2026) (amending Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E) (India)) (hereinafter IT Amendment Rules, 2026); see Bhardwaj & Goyal, *supra* note 1, at 123.

³ Bhardwaj & Goyal, *supra* note 1, at 124–25.

⁴ Vattem Murali Krishna, *Deepfakes and the Indian Constitution: Rethinking Privacy, Reputation and Freedom of Expression in the Generative AI Era*, 2 INT'L J. CREATIVE & OPEN RSCH. ENG'G & MGMT. no. 9, at 1, 2 (Sept. 2026); Abhishek Singh Parmar, *Ethical Labyrinth of Artificial Intelligence: A Legal Analysis in Light of Deepfakes*, LIVE LAW (June 18, 2026, 3:00 PM IST), <https://www.livelaw.in/articles/ethical-labyrinth-artificial-intelligence-legal-analysis-deepfakes-538193> (listing uses in entertainment, education, accessibility, and the arts).

⁵ Krishna, *supra* note 4, at 1–2.

⁶ Tisha T., *Regulating Deepfakes in India: A Constitutional and Criminal Law Analysis in Artificial Intelligence World*, 6 INT'L J. ADVANCED LEGAL RSCH. no. 4 (May 2026), ch. 1, § 1.1, ch. 6, § 6.5; Bhardwaj & Goyal, *supra* note 1, at 126.

⁷ Tisha T., *supra* note 5, ch. 1, § 1.1; Parmar, *supra* note 3.

⁸ Parmar, *supra* note 3.

the generated data is authentic; the generator learns through this process until it becomes almost impossible to differentiate between the generated data and real data.⁹ Known types of deepfake videos include face swaps, lip-syncing, "puppeteer" manipulation of the subject's motion, voice cloning, and avatar generation.¹⁰

Sexual themes predominate in the abuse cases. According to the 2019 Deeptech research used as evidence by Indian researchers, 96% of the deepfakes discovered by the organisation were pornographic.¹¹ Indian researchers agree that women are the main victims.¹² Other forms of harm are voice cloning aimed at deceiving relatives and authorities, false information about politicians, and misleading messages which fuel communal tensions; Swati, for example, discusses how viral manipulated messages trigger mob attacks in India, and predicts that deepfakes will only make things worse.¹³ The mere existence of deepfakes allows genuine evidence to be branded as fake, what Citron and Chesney describe as the "liar's dividend."¹⁴

III. CONSTITUTIONAL ASPECTS

A. Privacy, Dignity and Reputation under Article 21

Privacy is a fundamental right under Article 21, as decided by a Bench of nine judges in Justice *K.S. Puttaswamy (Retd.) vs. Union of India*,¹⁵ which is based on principles of dignity, autonomy, and liberty and involves informational self-determination. Deepfakes involve exactly this aspect of a right wherein the face, voice, and bodily image of a person are disassembled, digitised, and re-appropriated without consent. According to Krishna, there are three elements that come into play: informational privacy, decisional autonomy of one's own identity and "privacy of personality" concerning one's image and dignity.¹⁶ Reputation too is covered by Article 21 of the Constitution, which recognised reputation as an aspect of dignity when validating criminal defamation.¹⁷

Two limitations need mentioning here. First, while *Puttaswamy* was decided in the context of government surveillance and the Aadhaar system, it is still early days on how the decision

⁹ Ian J. Goodfellow et al., *Generative Adversarial Nets*, 27 *Advances Neural Info. Processing Sys.* 2672 (2014); Tisha T., *supra* note 5, ch. 2, § 2.4.

¹⁰ Parmar, *supra* note 3; Tisha T., *supra* note 5, ch. 2, § 2.3.

¹¹ Henry Ajder et al., *The State of Deepfakes: Landscape, Threats, and Impact* (Deeptech 2019); *see* Parmar, *supra* note 3.

¹² Tisha T., *supra* note 5, ch. 5, § 5.8; Bhardwaj & Goyal, *supra* note 1, at 126.

¹³ Swati, *Deepfakes and the Right to Privacy: Analysing Constitutional Restrictions under Article 19(2)*, 8 *Int'l J.L. Mgmt. & Human.* 1612, 1615–16 (2025).

¹⁴ Danielle Keats Citron & Robert Chesney, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 *Calif. L. Rev.* 1753, 1785–86 (2019); *see also* Tisha T., *supra* note 5, ch. 2, § 2.6.

¹⁵ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).

¹⁶ Krishna, *supra* note 3, at 3.

¹⁷ *Subramanian Swamy v. Union of India*, (2016) 7 SCC 221 (India).

might apply to a deepfake made by one private individual against another. In this regard, Bhardwaj and Goyal consider the precedent *R. Rajagopal v. State of Tamil Nadu*¹⁸, wherein a privacy interest in one's name, image, and life story had been acknowledged, as being the more relevant precedent.¹⁹ Secondly, even as *Kaushal Kishor v. State of Uttar Pradesh*²⁰ eases the horizontality question by stating that fundamental rights under Articles 19 and 21, under certain circumstances, can be made applicable against non-state entities and that there can be a positive obligation on the part of the State to protect such rights.²¹

B. Expression and Its Reasonable Restrictions under Article 19

Synthetic media can be used as a means of expression. Article 19(1)(a) permits its use for satire, parody, creative, and journalistic reasons. The latter includes the right to receive information and digital communication.²² The right is not unqualified, though. Article 19(2) allows restrictions on this freedom if done reasonably to protect interests, among others, of the sovereignty and integrity of India, security of the State, friendly relations with foreign States, public order, decency or morality, contempt of court, defamation, and incitement to an offence.²³ The former would involve sexually explicit content, the latter would involve content depicting criminality, and the last one would involve communal violence.²⁴

Two principles are important regarding this are: first, the limitation should be within the scope of one of the heads mentioned. Section 66A of the Information Technology Act was declared invalid in *Shreya Singhal* because it criminalised speech which is only annoying or offensive and thus is vague and intimidating and draws a distinction between discussion and advocacy on one hand and incitement on the other.²⁵ Secondly, the public order test needs a closer connection than disturbance of law and order. This principle was enunciated in *Arun Ghosh v. State of West Bengal*²⁶. Similar care has to be taken with respect to the head “decency or morality” although Swati relies on *Ranjit D. Udeshi v. State of Maharashtra*.²⁷

¹⁸ *R. Rajagopal v. State of Tamil Nadu*, (1994) 6 SCC 632 (India).

¹⁹ Bhardwaj & Goyal, *supra* note 1, at 125–26

²⁰ *Kaushal Kishor v. State of Uttar Pradesh*, (2023) 4 SCC 1 (India)

²¹ Tisha T., *supra* note 5, ch. 3, § 3.1 n.16.

²² *Shreya Singhal v. Union of India*, (2015) 5 SCC 1 (India); *Sec'y, Ministry of Info. & Broad. v. Cricket Ass'n of Bengal*, (1995) 2 SCC 161 (India); Krishna, *supra* note 3, at 3–4; Tisha T., *supra* note 5, ch. 3, § 3.3.

²³ India Const. art. 19, cl. 2; Swati, *supra* note 15, at 1613–14.

²⁴ Tisha T., *supra* note 5, ch. 3, § 3.4.

²⁵ *Shreya Singhal*, *supra* note 22; Krishna, *supra* note 3, at 3–4.

²⁶ *Arun Ghosh v. State of West Bengal*, (1970) 1 SCC 98 (India); see Swati, *supra* note 15, at 1615.

²⁷ *Ranjit D. Udeshi v. State of Maharashtra*, A.I.R. 1965 S.C. 881 (India); *Aveek Sarkar v. State of West Bengal*, (2014) 4 SCC 257 (India); see Swati, *supra* note 15, at 1616.

C. Equality under Article 14 and Article 15

The issue of non-consensual sexual deepfakes targets predominantly women, and thus is a gender-based abuse under Article 15(1) where Article 15(3) allows for special protection of women.²⁸ However, Article 14 warns against formulating a law that would leave out other victims. The provisions against sexual harassment, voyeurism, stalking, and insult to modesty contained in BNS target women as victims. This means men and transgender victims of sexual deepfakes lack similar protection²⁹. There should be a gender-neutral offense of deepfake but with aggravating circumstances of the sexual nature of the crime.

D. Proportionality Principle

Modern Dental College v. State of Madhya Pradesh expounded on proportionality as a four-fold test that includes a legitimate objective, a rational relationship, necessity (the least restrictive and most effective means), and proportionality as a balancing between the right and the objective sought to be accomplished. Puttaswamy requires that the infringement of privacy must be legal, legitimate and proportionate.³⁰ For a criminal prohibition, there must be a clear definition, one of the legitimate aims listed in Article 19(2) and 21 (such as the protection of reputation, the protection of dignity, public order, elections or from fraud), and that no other less restrictive means of achieving those aims exists (such as labelling, civil action).³¹

IV. CRIMINAL LIABILITY UNDER CURRENT FRAMEWORK

A. Personation and Forgery

In considering how to respond to a deepfake, prosecutors will first look at the criminal acts that come closest to what has taken place. Cheating by personation under section 319 of the BNS occurs where a voice or video that has been forged induces the victim to hand over property, as in cases of family emergency or “digital arrest.”³² However, impersonation is one form of cheating under section 318, which requires deception resulting in an act being induced by the deceived individual.³³

Forgery is a more complex problem. The definition of “document” in the BNS includes

²⁸ Bhardwaj & Goyal, *supra* note 1, at 126; India Const. art. 15, cls. 1, 3.

²⁹ Bhardwaj & Goyal, *supra* note 1, at 127; Parmar, *supra* note 3 (section on amendment of the penal code).

³⁰ Puttaswamy, *supra* note 17; *Modern Dental Coll. & Rsch. Ctr. v. State of Madhya Pradesh*, (2016) 7 SCC 353 (India); see Tisha T., *supra* note 5, ch. 3, § 3.4.

³¹ Krishna, *supra* note 3, at 2, 12.

³² Bhardwaj & Goyal, *supra* note 1, at 126; Bharatiya Nyaya Sanhita, 2023, No. 45 of 2023, §§ 318–319 (India) (hereinafter BNS).

³³ Bhardwaj & Goyal, *supra* note 1, at 124.

electronic records, so a fabricated video produced as a genuine record, say, in a marriage or employment case, can be said to be forged, and forgery that is done with the intent to defame others is dealt with in s. 336(4).³⁴ However, forgery law has always been about falsehood about the maker of a document, rather than mere falsehood in the contents of the document, so it is questionable whether a completely fabricated video “pretends” to be a record made by the person depicted.³⁵

B. Defamation, Intimidation and Sexual and Public-Order Offences

"Visible representation" is the language used in criminal defamation under s. 356 for the imputation, making it appropriate for reputational deepfakes.³⁶ Nevertheless, it has additional drawbacks. According to Bhardwaj and Goyal, criminal defamation is a bailable and compoundable offence that necessitates publishing an untruth. Damage that is mostly finished hours after the distribution is incompatible with this.³⁷ As mentioned above, Krishna's seven-part test, which includes whether the matter is presented as a fact, whether the matter relates to an identifiable person, whether it is substantially a false statement, whether the publisher of the matter was aware or ought reasonably to have been aware that the matter was false, whether there was harm cognizable in law resulting from the statement, whether any exception or lawful justification applied, and whether the restriction was proportionate to the harm, could be a way for defamation law to distinguish between deception and satire³⁸. It is, however, not the requirement of the statutory provision.

Sections 74, 75, 77, 78, and 79, which deal with assault on modesty, sexual harassment, voyeurism, stalking, and insult to modesty respectively, pertain to the sexual deepfake issue.³⁹ These sections were created after the report of the Justice Verma Committee on the gang rape in 2012 and they did not envisage any synthetic images.⁴⁰ Section 77 is about the making or publishing of an image of a real private activity, but does not make any reference to an image depicting nothing⁴¹. Section 294 deals with obscenity and is concerned with the circulation of obscene material rather than its private production. Sections 196 and 152 might be applicable in case of a deepfake used for incitement of communal animosity or for sovereignty and

³⁴ BNS, *supra* note 33, §§ 335–336; Bhardwaj & Goyal, *supra* note 1, at 125–27.

³⁵ *Md. Ibrahim v. State of Bihar*, (2009) 8 SCC 751 (India).

³⁶ BNS, *supra* note 33, § 356(1); Bhardwaj & Goyal, *supra* note 1, at 127.

³⁷ Bhardwaj & Goyal, *supra* note 1, at 130.

³⁸ BNS, *supra* note 33, § 351; Bhardwaj & Goyal, *supra* note 1, at 127.

³⁹ BNS, *supra* note 33, §§ 74–75, 77–79; Parmar, *supra* note 4

⁴⁰ Bhardwaj & Goyal, *supra* note 1, at 126.

⁴¹ Bhardwaj & Goyal, *supra* note 1, at 128–30.

integrity of India.⁴²

C. The Information Technology Act and the POCSO Act

There are parallel provisions for offences under the Information Technology Act, and the police make First Information Reports under both legislations for the same act.⁴³ Section 66C punishes fraud or cheating with the help of electronic signature, password, or other unique identification features; section 66D punishes cheating by personation through a computer system; and section 66E punishes capturing and publishing images of a private part. Sections 66C to 66E were inserted in 2008 to cover email scams, fake online identities, and espionage, but not synthetic media.⁴⁴ The suitability of this legislation is inconsistent in nature. Whether face and voice are “unique identification features” is not clear; section 66D carries forward the cheating element; and section 66E refers to capture of images, which cannot be of a synthetic nature.

Sections 67, 67A and 67B, which make it an offence to publish or transmit obscene material, sexually explicit material and material showing children engaged in sexually explicit acts respectively, constitute the primary law to be invoked in cases of unconsented synthetic intimate material.⁴⁵ As it requires publication and transmission, this law does not extend to the case of an offender who may create and store such material but fails to disseminate it. Where the subject of the act is a minor, then Sections 13 and 15 of the Protection of Children from Sexual Offences Act, 2012 will be applicable for simulating sexual acts and storing pornographic material.⁴⁶

V. JUDICIAL INTERPRETATION

The most refined judicial answer has been in civil rather than criminal surroundings. Delhi High Court Judgements have come in addressing the issue of synthetic misappropriation of identity, in the wake of the filing of lawsuits relating to personality and publicity rights. The basis of this doctrine is provided by *Rajagopal and Titan Industries Ltd. v. Ramkumar Jewellers*, the landmark case that laid down the common law right of publicity in India.⁴⁷ In

⁴² BNS, *supra* note 33, §§ 152, 196, 294; Parmar, *supra* note 4 (section on the BNS); Swati, *supra* note 14, at 1615–16.

⁴³ Information Technology Act, 2000, No. 21 of 2000, §§ 66C–66E, 67, 67A, 67B (India); Bhardwaj & Goyal, *supra* note 1, at 127.

⁴⁴ Bhardwaj & Goyal, *supra* note 1, at 125.

⁴⁵ Bhardwaj & Goyal, *supra* note 1, at 127; Tisha T., *supra* note 6, ch. 4, § 4.3.

⁴⁶ Protection of Children from Sexual Offences Act, 2012, No. 32 of 2012, §§ 13–15 (India); Parmar, *supra* note 4 (section on the POCSO Act).

⁴⁷ Bhardwaj & Goyal, *supra* note 1, at 126, 128; *Titan Indus. Ltd. v. Ramkumar Jewellers*, 2012 SCC OnLine Del 2382 (India).

the case of *Anil Kapoor v. Simply Life India*, prevented from having his name, voice and image used without permission, including to create deepfakes with AI, the protection was extended to those who were yet to infringe.⁴⁸ The protection afforded to Amitabh Bachchan against the abuse of his name, image, and voice was subsequently broadened to cover future AI-generated images and sounds, and in *Jackie Shroff v. The Peppy Store*, the likeness of the actor was prohibited from being used in AI and chatbot applications.⁴⁹

The developments reveal two weaknesses in the criminal law. The first is the absence of any parallel criminal law: there is nothing analogous under sections 319, 336, 356 or 77 of the BNS for deepfakes, and the interpretative issues raised above have not yet been resolved.⁵⁰ Second, these measures are also inequitable in that they can only be enforced on a plaintiff whose lawsuit is commercial in nature, but who cannot afford to file such an action, while the typical fraud victim or intimate-image victim remains trapped in a slow, cumbersome criminal case.⁵¹ Civil redress is good, but it is not a substitute for criminal deterrence.

VI. DOCTRINAL AND ENFORCEMENT CHALLENGES

A. Conduct, Fault and Classification

Each one of these provisions has been crafted in a different context altogether, and there will be costs associated with its extension. Private production and storage of a non-consensual synthetic intimate image, but not public dissemination thereof, would seem to fail both requirements set out in section 336, which requires the intent to treat the document as authentic, as well as section 77.⁵² The definition of the requisite mens rea remains unspecified. As Krishna suggests, a consideration of what harms the content causes, to whom, by what means, and with what degree of intent or recklessness makes for a good beginning of a statute.⁵³ There is no shortage of procedural issues here either.

B. Evidence

Bhardwaj and Goyal state that Section 63 of the Bharatiya Sakshya Adhiniyam, 2023 applies to electronic data, but does not provide any mechanism for presuming or shifting the burden of

⁴⁸ *Anil Kapoor v. Simply Life India*, CS (Comm) 652/2023 (Del. High Ct. Sept. 20, 2023) (India); Bhardwaj & Goyal, *supra* note 1, at 128.

⁴⁹ *Amitabh Bachchan v. Rajat Nagi*, CS (Comm) 819/2022 (Del. High Ct. Nov. 25, 2022) (India); *Jackie Shroff v. The Peppy Store*, CS (Comm) 389/2024 (Del. High Ct. May 15, 2024) (India); Bhardwaj & Goyal, *supra* note 1, at 128.

⁵⁰ Bhardwaj & Goyal, *supra* note 1, at 128–29.

⁵¹ Bhardwaj & Goyal, *supra* note 1, at 128–29.

⁵² Bhardwaj & Goyal, *supra* note 1, at 130.

⁵³ Krishna, *supra* note 4, at 2.

evidence for data generated by artificial intelligence.⁵⁴ It is thus up to the court to establish authenticity by expert witnesses. Krishna cautions against adopting a stance in either manner, saying that although courts cannot assume the veracity of any compelling evidence, they also cannot reject acceptable evidence just because it is purported to be a deepfake.⁵⁵

C. Attribution and Allocation of Liability

There are some cybercrime divisions that are not trained in forensic and AI skills, and they use encrypted communications and servers overseas.⁵⁶ While the three-hour requirement of the Information Technology Act vis-à-vis offshore resources is still up for debate, it extends the reach of the jurisdiction to a crime committed abroad involving a computer system in India.⁵⁷ Moreover, the criminal law is based on the purpose and actions of people, but the harms can be caused by many actors, including developers, data set suppliers, users, distributors, and platforms.⁵⁸ Also, the duty under BNS has no legal nexus with the duty under the Rules.⁵⁹

VII. Comparative Analysis

A transparency regime has been established in the EU. Article 50 of the Artificial Intelligence Act mandates that the manufacturer must make it possible to identify a generative system by using a machine-readable format and requires disclosure when deepfakes are used for purposes other than artistic, satirical or fictional use.⁶⁰ There is no criminalisation for creating the deepfake that can cause harm in the Act. In the United States, limited by the First Amendment, regulation comes through application. Its federal TAKE IT DOWN Act, addressing the issue of non-consensual intimate images, both real and AI-made, applies to individual liability and a notice-and-takedown scheme enforced by the Federal Trade Commission within 48 hours.⁶¹ States have laws pertaining to voice and likeness, such as Tennessee, and election deepfakes. For example, California's AB 730 (2019) prohibits the distribution of substantially false information about candidates within 60 days of an election.⁶² The Chinese approach, which has been attacked for its detrimental consequences on freedom of expression and increased

⁵⁴ Bharatiya Sakshya Adhiniyam, 2023, No. 47 of 2023, § 63 (India); Bhardwaj & Goyal, *supra* note 1, at 130–31.

⁵⁵ Krishna, *supra* note 4, at 10–11.

⁵⁶ Tisha T., *supra* note 6, ch. 4, § 4.4, ch. 6, § 6.2.3; Bhardwaj & Goyal, *supra* note 1, at 131.

⁵⁷ Information Technology Act, *supra* note 46, § 75; Bhardwaj & Goyal, *supra* note 1, at 131.

⁵⁸ Tisha T., *supra* note 6, ch. 6, § 6.2.4.

⁵⁹ Bhardwaj & Goyal, *supra* note 1, at 130.

⁶⁰ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence, 2024 O.J. (L 1689) 1, art. 50; Bhardwaj & Goyal, *supra* note 1, at 129.

⁶¹ TAKE IT DOWN Act, Pub. L. No. 119-12, 139 Stat. 55 (2025); Bhardwaj & Goyal, *supra* note 1, at 130.

⁶² Ensuring Likeness, Voice, and Image Security Act, Tenn. Code Ann. § 47-25-1101 *et seq.* (2024); Cal. Elec. Code § 20010 (West); Parmar, *supra* note 4 (section on Election Commission regulations); Tisha T., *supra* note 6, ch. 6, § 6.4.1.

monitoring, employs provider responsibility, required labelling, and government control.⁶³

In contrast to the Indian design, where the BNS does not adequately cover the perpetrator and the Rules cover the platform without any reference back to each other, the United States design shows the advantage of pursuing the most harmful acts through a perpetrator offence paired with a platform process⁶⁴. The European design demonstrates that providers can be subject to labelling and provenance rules without making any technology illegal. Additionally, China's design emphasises the cost of free speech when state-oriented regulation is used.

VIII. RECOMMENDATION FOR REFORMS

Reform should be initiated by way of a restricted offence of deception through artificial impersonation. The BNS should criminalise, as an addition to the Information Technology Act under Section 66, any creation or dissemination of synthetic audio-visual or textual impersonation of an identifiable individual without his or her permission if it has the capacity to deceive a reasonable person about its veracity, and it was created with intent or knowledge that it would harm someone's reputation, property, or dignity.⁶⁵ This offence should be based on consent and deception, but not on artificial intelligence and should not apply to satire, parody, journalism, research, or consensual material.⁶⁶

Gender-neutral graded levels must then come next. Sanctions should be harsher, and the infraction should be cognizable; that is, police action can be conducted without the magistrate's previous consent in cases involving sexually explicit content, children, fraud or extortion, or any type of election⁶⁷. Due to the gravity of the repercussions and the risks of possible publication, non-dissemination will only apply to the categories that are sexually explicit and child-relevant.

Equivalent adjustments must be made to the law of evidence. According to Bhardwaj and Goyal, the law should acknowledge a rebuttable presumption that content lacking the provenance metadata or labelling required by the Rules but displaying characteristics that are suggestive of AI development according to a known forensic process is artificial.⁶⁸ This makes sense if the presumption can remain rebuttable and based on expert standards so as not to contribute further to the liar's dividend, and if courts create processes for authentication of

⁶³ Provisions on the Administration of Deep Synthesis of Internet Information Services (promulgated by the Cyberspace Admin. of China, Nov. 25, 2022, effective Jan. 10, 2023) (China); Tisha T., *supra* note 6, ch. 6, § 6.4.3.

⁶⁴ Bhardwaj & Goyal, *supra* note 1, at 130.

⁶⁵ Bhardwaj & Goyal, *supra* note 1, at 131.

⁶⁶ Krishna, *supra* note 4, at 7, 9.

⁶⁷ Krishna, *supra* note 4, at 9–10; Bhardwaj & Goyal, *supra* note 1, at 131.

⁶⁸ Bhardwaj & Goyal, *supra* note 1, at 132.

alleged deepfakes.⁶⁹ The criminal and regulatory laws must also converge in that a failure by a platform to label or act in violation of the Rules must be admissible as evidence of constructive notice.⁷⁰ Protections of notice, explanation, human intervention, appeal, and restoration of legitimate material, judicial review of blocking involving significant political and journalistic expression, regular transparency reporting, and traceability, which must identify the source of illegitimate material without keeping an eye on lawful users, must all be included in the removal obligations.⁷¹

Finally, there has to be a complaint process with a time limit, development of evidence, and compensation, while also training the investigators and forensic infrastructure and increasing the public's awareness of synthetic media.⁷²

IX. CONCLUSION

All these principles that are required to control deepfakes are also available in the Constitution of India. In the first place, the right to respect for private life, respect for dignity and respect for reputation are guaranteed by Article 21. In the second place, Article 19(2) allows restrictions to be imposed, but only to the extent that they are reasonable on the basis of certain conditions. In the third place, Article 14 and Article 15 require equality and an action in response to gender-related harm. In the fourth place, proportionality should guide the selection of the means. The current legislation provides some answers to many of the problems associated with deepfakes, but the coverage limits, inability to keep pace with the pace of digital harm, and lack of proof and attribution requirements are still concerns. The 2026 Rules govern the platforms, while the Rules governing offenders will be different. If the crime of "misleading synthetic personation" could be restricted, controlled and differentiated between aggravated and gender-neutral varieties, it would be possible to penalise the crime without penalising the innovation. It would also have to adhere to an evidentiary norm and procedural safeguards.

⁶⁹ Krishna, *supra* note 4, at 10–11.

⁷⁰ Bhardwaj & Goyal, *supra* note 1, at 132.

⁷¹ Krishna, *supra* note 4, at 10, 12.

⁷² Tisha T., *supra* note 6, ch. 4, § 4.5, ch. 6, § 6.6; Krishna, *supra* note 4, at 12.