

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IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines.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.

DEEPFAKES, CONSENT, AND SEXUAL OFFENCES UNDER INDIAN CRIMINAL LAW: ARE EXISTING LEGAL FRAMEWORK ADEQUATE?

AUTHORED BY - SUMBUL RAZA

BA.LLB/ SEM 4th

SCHOOL OF LAW HAMDARD INSTITUTE OF LEGAL STUDIES AND RESEACH

JAMIA HAMDARD UNIVERSITY

INDEX

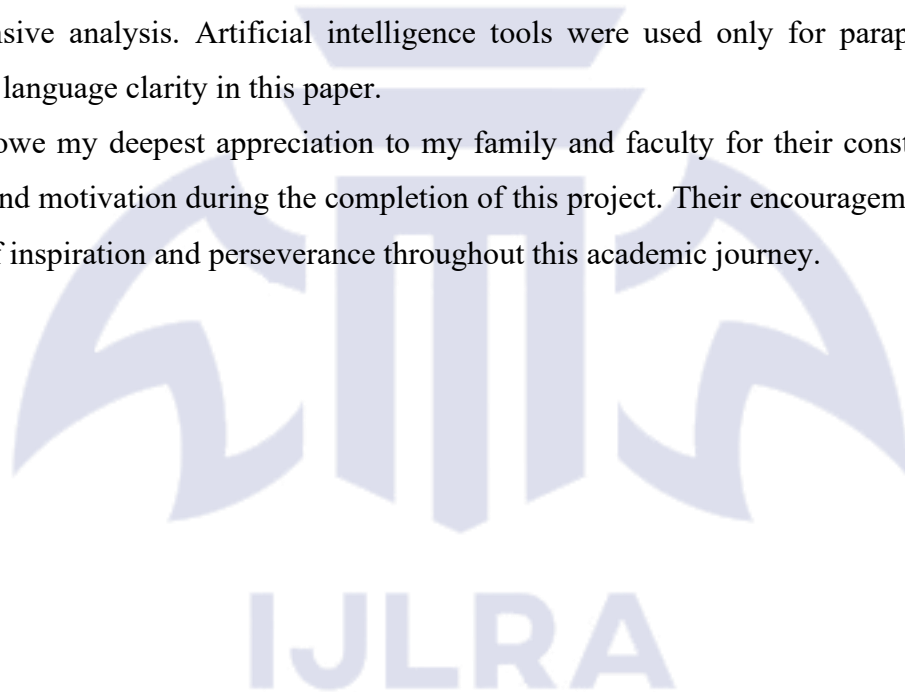
S.NO.	CONTENT
1.	Acknowledgment
2.	Group Member's Contribution
3.	Abstract
4.	Introduction
5.	Types of deepfake
6.	Application of deepfake
7.	Consent in Criminal law
8.	Deepfakes and Sexual offences
9.	IT Act, 2000
10.	BNS, 2023
11.	DPDP Act, 2023
12.	Regulatory and Institutional Framework
13.	Constitution of India
14.	Recommendations
15.	Conclusion
16.	Reference

ACKNOWLEDGEMENT

I would like to express my heartfelt gratitude to Jamia Hamdard University and the Department of Law, HILSR, for providing me with the opportunity to undertake this project titled **"Deepfakes, Consent, and Sexual Offences under Indian Criminal Law: Are Existing Legal Frameworks Adequate?"**

I am also thankful to the university library and online academic resources that provided me access to authentic reference materials and scholarly works necessary for developing a comprehensive analysis. Artificial intelligence tools were used only for paraphrasing and improving language clarity in this paper.

Finally, I owe my deepest appreciation to my family and faculty for their constant support, patience, and motivation during the completion of this project. Their encouragement has been a source of inspiration and perseverance throughout this academic journey.



ABSTRACT

Deepfake technology has exploded over the past few years, driven by AI and machine learning resources. It's become possible to generate audio, images and videos that look and sound real but are totally fabricated. There are a lot of good things to do with this like entertainment, creative projects or new ways of communicating online. But deepfakes have also been used in some deeply disturbing ways. Creating content without someone's permission by using their face or body in pornographic scenes and they don't even know about it. This can ruin a person's reputation. Really hurt their mental health. It also invades their privacy in ways that're hard to fix.

It delves into what happens when people consent to a deepfake and what happens when they don't. Non-consensual deepfakes often fit the profile of a sexual offense, online harassment or so-called image-based sexual abuse. Indian criminal and cyber laws already cover things like obscenity, harassment and privacy but none of them specifically address deepfakes. There is simply too much gray area.

Keywords: Deepfake Technology, Artificial Intelligence (AI), Digital Sexual Violence, Reputational Harm, Deepfake pornography, Data Protection and Privacy Rights, AI Ethics and Governance.

INTRODUCTION

Deep Fake is a process where the face in the video of one person is replaced by another person's face to make it look like the new and target persons face goes together. They are created with the help of machine learning algorithms like **Generative Adversarial Networks (GANs)**. Generative Adversarial Networks were first talked about by Goodfellow et al in 2014.

Deepfakes use GANs which are of two types: A generator that makes some fake content, and a discriminator that then validates whether these contents are fake or real. Deepfakes and Generative Adversarial Networks trained on vast amounts of data can create exceptionally lifelike sounds and visuals¹.

Everyone heard about fake content, but Deepfake is a little different than what we usually have

¹ Johan Kietzmann, Ian P. McCarthy & Leyland Pitt, *Deepfakes: Trick or Treat?* 63 Bus. Horizons 135 (2020).

in mind. Such techniques mangle the original content to generate false information. Deepfake is used for tons of stuff like fake porn of popular personalities, wrong news, creating voices of politicians and the economic fraud. This is a popular technique in the film industry also. Traditionally, making fake voices or videos took more time and skill to do. Today anyone, with a computer and a good graphics card can easily make videos and pictures that look real.

People who are victims of non-consensual deepfake pornography suffer from term emotional pain, psychological distress and harm to their reputation. According to a report, all deepfake videos on the web were pornographic and made-up 96 percent according to the cybersecurity company Deeptrace. The majority of the deepfake videos used images of women without their consent. This is a problem because it is a form of gendered digital violence and image-based sexual abuse. Deepfake videos are being used in a bad way and it is mostly women who are being hurt by them². False videos and images that go viral can easily damage individuals and this has been an issue of concern to the masses of late³. This is why public awareness campaigns are really important. We also need systems to detect abuse and rules to prevent it.

Fake news, fraud, and transmission of hoaxes are also generated with the help of the technique. Deepfakes are not specifically addressed by the BNS, despite its updated terminology and rearranged offenses. However, several provisions dealing with sexual offences, privacy violations, and harassment can be interpreted to cover such conduct.

TYPES OF DEEPPFAKE

1. Video deepfakes:

Fake video is a face from other person is putted over the Body of someone and their expression is modified. The majority of video deepfakes are created using a technique to swap faces so that it appears as though one person's face is moving and flexing on another person's body. Video deepfakes are great for entertainment or creativity but can also be weaponized in far more harmful ways.

² Henry Ajder, Giorgio Patrini, Francesco Cavalli & Laurence Cullen, *The State of Deepfakes: Landscape, Threats, and Impact* (Deeptrace, 2019), <https://culturereframed.org/library-article/the-state-of-deepfakes-landscape-threats-and-impact/>.

³ Claire Wardle & Hossein Derakhshan, *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making* (Council of Eur., 2017).

2. Audio deepfakes:

Audio deepfakes are like voices that sound just like the real person. These models use techniques and computers to learn from a lot of recordings of the person's voice. They can make audio that sounds really close to the way the person talks with the tone and accent. There are serious risks involved.

3. Image Deepfakes:

Image deepfakes are edits of images where they change facial expressions, background details or whole subjects. it does not really require any computation, it has the potential for various uses, either for the purpose of spoofing the identity of a particular individual on the social media platform.

4. Multimodal Deepfakes:

Recent breakthroughs have resulted in the production of multimodal deepfakes, which combine video, audio, and text in one output. As an example, a multimodal deepfake could produce a video where someone is heard to speak words that were synthesized to sound like theirs, including facial features in the correct order and motions as well as other possible background information in said video. Such a comprehensive method to deepfakes renders them more believable and harder to detect⁴.

APPLICATION OF DEEPPFAKE

Deepfake technology has so many uses for good or bad. But it is often misused for evil reasons. Deepfake poses a great threat to people who actively use social media. However, if handled correctly this could yield many benefits.

1. Negative Application:

There are many reasons why people make Deepfake content. It is sometimes done for fun, but it can also be malicious in nature like revenge, blackmail, identity theft and many more. There are thousands of Deepfake videos, with many being adult videos of women posted without their permission. The most common use of Deepfake technology is to create pornography featuring well-known actresses. This trend is increasing daily,

⁴ Nilufer Bhateja, *Emerging Technologies and Law: Legal Status of Tackling Crimes Relating to Deepfakes in India*, SCC Online Blog (Mar. 17, 2023), <https://www.sconline.com/blog/post/2023/03/17/emerging-technologies-and-law-legal-status-of-tackling-crimes-relating-to-deepfakes-in-india/>.

particularly among Hollywood actresses. In 2018, software emerged that could make a woman appear nude with a single click, and it quickly went viral for harmful reasons to harass women. Another harmful use of Deepfake is making fake videos of world leaders and politicians, posing a significant threat to global peace. Almost every world leader has been targeted by fake videos, including Barack Obama, Donald Trump, even Facebook founder Mark Zuckerberg has faced similar situations⁵.

Among damages are:

harm to one's reputation, trauma to the mind, exploitation of sexuality, extortion and blackmail, false information about politics.

2. Positive Application:

While misused for malicious intent, such a technology can also have positive applications in multiple industries. The construction of deepfakes is no longer the domain of specialists.

- Entertainment — A voice (or likeness) can be used in a movie for artistic purposes, or to achieve continuity when the original performer is unavailable.
- E-commerce - An online retailer may allow customers to virtually try on clothes by using their likeness.
- Communication - Speech synthesis and facial manipulation allow a user to appear as if they are speaking a foreign language in a natural manner⁶.

CONSENT IN CRIMINAL LAW

While the BNS supersedes the Indian Penal Code, with respect to this specific offense it still retains virtually the same principle of consent. Consent still must be voluntary, informed and given without fear, coercion or deception.⁷

Digital deepfakes make it difficult to determine whether someone consented, because:

- The thing that is shown might not have even happened.
- Just because someone agreed to have their picture taken it does not mean they agreed to have it changed with intelligence.

⁵ Bahar Uddin Mahmud & Afsana Sharmin, *Deep Insights of Deepfake Technology: A Review*, 5 DUJASE 13, 14 (2020).

⁶ U.S. Gov't Accountability Off., *Science & Tech Spotlight: Deepfakes*, GAO-20-379SP (Feb. 20, 2020), <https://www.gao.gov/assets/gao-20-379sp.pdf>.

⁷ Bharatiya Nyaya Sanhita, 2023, No. 45 of 2023, § 28 (India).

- Just because someone agreed to have a picture taken for use it does not mean they agreed to have it shared with the public.

The NCW (National Commission for Women) also pointed out that deepfakes do not fit within the current Indian criminal law system and specifically, the BNS (Indian Criminal Law and Procedure) does not currently define deepfakes as a separate crime, creating a gap in the legal system regarding consent issues in relation to AI-generated materials.⁸

In the context of sexual offences, it was clarified that consent in sexual offences requires clear voluntary agreement⁹.

The idea of consent in law is now affected by digital things. A person's digital identity, including their face, voice and personality is now considered a part of their information. In **Justice K. S. Puttaswamy v. Union of India**, the Supreme Court held that individuals possess control over their private information — including their digital likeness. In other words, just because someone had a photo of them taken, that does not somehow give anyone the rights to use it in any manner.

Mrinal Satish, a legal scholar, has argued that rape law in India should protect a woman's **right to choose**, not test whether she "fought hard enough." And when applied to deepfakes, the law should focus on whether her **sexual autonomy was violated**, not whether there was physical force¹⁰. If someone creates a sexual deepfake without her consent, even without touching her, her **sexual autonomy** (her right to decide about her own body and sexual identity) is violated.

Valid consent:

Deepfakes made with the clear, informed, and voluntary consent of the individual do not on their own constitute an offence under the BNS. The principle of Informational Control was previously recognized in the case of **R. Rajgopal v. State of Tamil Nadu**. Here, the court recognized the individual's right to control the publication of their information¹¹.

Limitations of consent:

⁸ National Commission for Women, *NCW Recommends Legal Definition and Penalties for Deepfake Abuse Under Bharatiya Nyaya Sanhita* (India).

⁹ Bharatiya Nyaya Sanhita, 2023, No. 45 of 2023, § 63 Explanation 2 (India).

¹⁰ Mrinal Satish, *Consent and the Indian Penal Code*, 50 *Econ. & Pol. Wkly.* 60 (2015).

¹¹ *R. Rajagopal v. State of Tamil Nadu*, (1994) 6 S.C.C. 632 (India).

- **Section 66E** makes it a criminal offense to capture or transmit private areas of a person's body without their consent. Deep fake sexual images could also be considered to come within this provision if consent is lacking or not valid¹².
- **Section 67 and 67A** cover the publication of obscene or sexually explicit material on the internet. Consent to making the material may not be sufficient to negate liability for distributing it¹³.

Similarly, public policy restricts consent in cases involving obscenity or exploitation. In State of **Maharashtra v. Mohd. Yakub**¹⁴, the court emphasized that criminal law protects societal interests beyond individual waiver. Thus, even if an adult consents to deepfake manipulation, someone shares it in a way that was not agreed on or uses it in a way they can still get in trouble for it. The law can hold people responsible for deepfake manipulation even if the person, in the deepfake said it was okay.

DEEPAKES AND SEXUAL OFFENCES

The emergence of deepfake technology has created a dangerous new form of digital sexual abuse. The initial public response to artificial intelligence recognized its potential for creative work, but people started using it to create non-consensual sexual content which turned AI into a tool for exploitation. Deepfake technology enables sexual offenses through its ability to create unauthorized visual content that uses a person's facial features in explicit materials. The technology-driven evolution of this abuse creates a new form of image-based sexual violence because it allows abusers to spread victims' private images without their consent.

Deepfake sexual content makes up a large portion of online deepfake material which targets women more than other groups (Westerlund, 2019). Research on deepfake websites shows that over 90% of available deepfake videos show women in non-consensual sexual situations (Kietzmann et al., 2020). The distribution of this pattern shows that digital societies maintain existing gender-based power imbalances. The technology objectifies women while using digital identity reconstruction to erase their ability to give consent.

Things are worse in a country like India, with cultural and family norms adding to the plight of people who are victims of deepfake sexual content. Saving honour is paramount in Indian

¹² Information Technology Act, 2000, No. 21 of 2000, § 66E (India).

¹³ Information Technology Act, 2000, No. 21 of 2000, §§ 67–67A (India).

¹⁴ *State of Maharashtra v. Mohd. Yakub*, (1980) 3 S.C.C. 57 (India).

society and if somebody has been victimised, then that does not only affect the individual but their entire family and society. It can do so much damage even if the content is totally fake. Victims of being victimized can feel extremely lethargic, anxious, sad, etc., and can often think about killing themselves. The additional emotional pain created by the fear of being blamed by others and ostracized from society tremendously complicates things for a subject who has been victimized, creating a sense of total isolation from others, and no one to whom the victim can reach out. Furthermore, the impact of depictions of sexual violence against women through deep fake technology extends beyond the victim and will ultimately cascade through their family and community as well.

There have had, however, some high-profile incidents of the modification of images of female journalists, activists, and public figures in India. Often, this modification of images is the result of an individual's desire to seek revenge against a woman who articulates her opinion publicly; the intention is to create fear and punish. This represents a form of online harassment specifically aimed toward women (digital gender-based harassment), and when a woman's image has been further modified, it attacks not only her reputation, but it destroys her sense of identity as well as her dignity. The harm is real and it's not just about what people think of them, it's about who they are as a person¹⁵.

Understanding the seriousness of deepfake sexual offenses still depends on the consent question. Informed consent is violated even when people willingly exchange personal photos in private settings. This is especially true when those photos are later altered into explicit deepfakes. Consent is not a general permission to change technology or make it available to the public. Deepfakes take use of what is referred to as the "consent gap" in digital contexts, where current rules are unable to combat synthetic manipulation, as legal scholars stress.

India's laws cover issues like obscenity and online abuse through the Information Technology Act, 2000, and some sections of the Indian Penal Code; however, there is no complete legal structure to deal with the unique challenges presented by synthetic media created using artificial intelligence. In the current situation, victims may have difficulty obtaining proper justice due to a lack of mechanisms in place to enforce the relevant laws, identify those who

¹⁵ Robert Chesney & Danielle K. Citron, *Deepfakes and the New Disinformation War: The Coming Age of Post-Truth Geopolitics*, 98 Foreign Affs. 147 (2019).

violate them and/or remove content created outside of India. Consequently, when victims who suffer harm caused by synthetic media attempt to seek support and assistance in order to obtain justice and protection, they are frequently faced with barriers caused by a lack of responsiveness and/or support from the established organizations that are meant to assist victims; thus, victims often fail to achieve justice as a result, while the courts face the challenge of resolving the unique legal issues pertaining to this new category of cases.

The impact of personal trauma happens to not only happen to an individual but extends to everyone within our society as well. With the loss of trust will also be the increase in the difficulty of identifying which content is real and which content is fake in regards to digital content. This is especially true for explicit content that can easily be altered by someone who has even a minimal number of technical skills. The confusion created by this will often cause real victims of trauma to have difficulty proving they were harmed while allowing those who perpetrated the harm to escape consequence for their actions¹⁶. There has been discussion from researchers such as Vaccari and Chadwick regarding the impact of deepfake technology and the overall loss of trust in our ability to believe in what we see. This loss of trust in more conservative societies such as India which often places a significant value on the reputations of their society, can result in long-term negative consequences for the individual who is being victimized.

Digital media can exist permanently once released into the digital arena causing victims of trauma to experience repeated emotional pain. The survivor may continue to feel humiliated and ashamed for the rest of their life even if the content is successfully removed from one website. This is comparable to what has been called "digital immortality of harm," in which you are continuously reminded of a negative experience you had online and feel as though you are repeatedly going through the trauma. We must use a multifaceted strategy to address the issue of deepfake-enabled sexual harassment in India. First, we must ensure that non-consensually produced sexual images based on AI are legally recognized as a distinct crime. Secondly, we must fortify our technological defences, including AI-based detection technology. This will enable people to critically evaluate online content and create an environment that does not blame victims. This way, we can work towards creating a safer and more responsible online environment. The concept of "digital immortality of harm" refers to

¹⁶ Cristian Vaccari & Andrew Chadwick, *Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News*, 6 Soc. Media + Soc'y 1 (2020).

when a traumatic event or incident occurs to someone and continues to affect them because the digital space is permanent, and the harm continuously resurfaces or reoccurs. When people continue to experience trauma from a particular incident, the psychological burden they face can be very heavy.

In order to prevent this type of violent crime—AI-assisted (deepfake) sexual crimes—in India, a multi-dimensional approach is needed. First, the production and dissemination of sexually explicit non-consensual images produced by artificial intelligence must be acknowledged by our legal system as a distinct criminal offense. Second, in order to prevent these crimes, we must bolster our digital security (for example, by improving artificial intelligence detection technology). In order to foster a culture where people are capable of assessing and critically analysing the authenticity of digital media without participating in victim-blaming, it is necessary to raise awareness of deepfake technology through basic literacy education. We can contribute to the creation of a more moral and secure online community by doing this. In conclusion, the creation and dissemination of fake sexual imagery in India is proof of a fundamental, systemic inequality in the treatment of men and women, the fundamental shortcomings of the current digital security framework, and the lack of effective legislation to prevent such offenses. The damage is done to both the individual; however, the cumulative damage of these actions also relates to society/communities. To develop laws that enable human rights (freedom, dignity, and digital rights) within an environment of artificially intelligent platforms (AI), it is essential to see this from the human perspective¹⁷.

LEGAL LANDSCAPE IN INDIA

1. INFORMATION TECHNOLOGY ACT, 2000

The Information Technology Act, 2000 function as India's major legal structure for handling deepfake-related harms. While the Act was introduced before deepfake technology, its technology-neutral drafting allows several sections to be applicable to synthetic media cases.

Prominent Sections:

Section 66C: Identity Theft

Anyone who fraudulently or dishonestly exploits another person's password, electronic

¹⁷ Mika Westerlund, *The Emergence of Deepfake Technology: A Review*, 9 Tech. Innovation Mgmt. Rev. 39 (2019).

signature, or other distinctive identifying feature faces up to three years in prison and a fine of up to one lakh rupees.

Section 66D: Cheating by Personation

Whoever, using any communication device or computer resource cheats by pretending to be someone else, may also be required with imprisonment for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

Section 66E: Violation of Privacy

A person faces up to three years in prison, a fine of no more than two lakh rupees, or both if they willingly or knowingly capture, distribute, or transmit a picture of another person's private area without that person's agreement and in a way that breaches that person's privacy.

Section 67A: Sexually Explicit Content Transmission

A maximum punishment of seven years in prison and a fine of ten lakh rupees is imposed on anyone found guilty of publishing, transmitting, or sending electronically any content that comprises sexually explicit acts or conduct¹⁸.

Limitations:

1. The specific type of media technology termed “artificial” or “synthetic” is not mentioned by the law. Consequently, one has to interpret the provisions of general cybercrime to understand the law as it pertains to AI generated deepfake.
2. Many deepfakes can be legally created and be harmful or misleading, for example, they can be damaging to a person’s reputation, and can be created without falling under the legal category of “obscene”. Because of this, the spread of lies and damaging content is punishable under the law by something that isn’t legally categorized as “obscene”.
3. The law is concerned with the acts of dissemination, and reproduction of harmful content, as opposed to the acts that are designed to create or construct the content. Consequently, a person can be the sole creator of a deepfake, and as long as they don’t publish it, they won’t be criminally responsible¹⁹.

2.BHARITYA NYAYA SANHITA, 2023

The Bharatiya Nyaya Sanhita, 2023 does not expressly mention “deepfakes” or “AI-generated synthetic media.” Therefore, prosecution must rely on analogous offences.

¹⁸ Information Technology Act, 2000, No. 21 of 2000, §§ 66C, 66D, 66E, 67A (India).

¹⁹ Preksha Singh, *Deepfakes, Identity Theft, and the Dark Web: Legal Gaps in AI-Generated Fraud*, Int’l J. Civ. L. & Legal Rsch. (2025).

The following sections are most relevant.

1. Defamation Section 356 –

It occurs when a person makes or publishes any imputation about another individual with the intention to harm, or knowing that it is likely to harm, that person's reputation. The offence requires that the statement or allegation is about an identifiable person and harms their reputation in the eyes of society.

2. Forgery

Forgery provisions are under Chapter relating to false documents and electronic records.

Section 335 – Making a False Document

Defines what constitutes a "false electronic record."

Section 336 – Forgery

Punishes making a false document or electronic record with intent to cause damage or injury.

Section 340 – Forgery for Purpose of Cheating

Forgery committed specifically to cheat.

3. Cheating

Section 318 – Cheating

Whoever deceives a person and fraudulently or dishonestly induces them to:

- Deliver property, or
- Do/omit something causing harm.

Section 319 – Cheating by Personation

Cheating by pretending to be another person.

4. Criminal Intimidation

Section 351 – Criminal Intimidation

Threatening another person with:

- Injury to body
- Injury to reputation
- Injury to property

With intent to cause alarm or compel action.

5. Outraging Modesty (Sexual Deepfakes)

Section 74 – Assault or Criminal Force to Woman with Intent to Outrage Her Modesty

Requires:

- Assault or criminal force
- Against a woman
- With intent to outrage modesty

Section 75 – Sexual Harassment

Includes:

- Physical contact and advances
- Showing pornography against the will of a woman

Section 77 – Voyeurism

Observing or recording images of a woman involved in a private act without permission²⁰.

Challenges in Bharatiya Nyaya Sanhita

1. The BNS has no specific subsection that defines or criminalizes deepfakes. The authorities are forced to work with existing provisions that were not intended to cover such offences.
2. The offender's use of a VPN, use of an encrypted platform, or an overseas server located outside of India, cause challenges for investigative agencies in locating the original offender.
3. Forensic expertise is required to determine whether a video or audio is a deepfake. Courts do not have uniform standards for the admission of such digital evidence, causing a backlog in the court's business.
4. The law is concerned more with the punishment of the offender. There are few, if any, provisions that assist a victim in obtaining an expeditious removal of the material, or to provide a victim with the ability to sue for loss of reputation.
5. The absence of a definition for "deepfake" or "synthetic media" in the statute, and the use of these terms, may lead to a misinterpretation of the actions that constitute an offence²¹.

²⁰ Bharatiya Nyaya Sanhita, 2023, No. 45 of 2023, §§ 74, 75, 77, 318, 319, 335, 336, 340, 351, 356 (India).

²¹ N. R. Divyashree, *Deepfakes and Indian Criminal Law: Addressing the Gaps in Legal Protection*, Indian J. L. & Legal Rsch. (2025).

3.THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

India's legislative system for protection of personal data is provided in the Digital Personal Data Protection Act, 2023 (DPDP Act). Its provisions are applicable in the context of deepfakes, where AI generated content is created using an individual's likeness.

Notable Key parts of the Act include:

The Act Affirmative Action and Compliance require the processing of personal data only after obtaining a person's prior personal consent. Consent must be in a documented manner and the person must be able to revoke their consent at any point in time²². This is especially important in situations where a person's image or voice is used without permission to create a deepfake.

The Act gives persons the right to

(i) access (ii) edits or (iii) delete their personal information. This is particularly important in the right of a person who has been misappropriated to be a likeness in the deepfake. The provision in 'The Right to be Forgotten'²³ is available to the individual who requests to have their data erased and this is especially applicable to situations where synthetic media is used to infringe on people's private data.

The Act requires all data processors to take mappers and countermeasures to prevent use of data without permission and to counter any breaches of data. This includes the requirement to prevent misuse of data and this falls within the scope of preventing the unlawful creation of deepfakes. Data fiduciaries must handle the personal data in their possession in a transparent manner and explain to the individual how the data is processed.

Limitations and Scope for Improvement:

Despite the enviable glory of having a DPDP Act, it needs to be stressed that there are specific challenges raised by deepfakes which will require targeted response, such as:

1. **Enforcement of Technology:** Other techniques including digital watermarking, and blockchain that captures/ validates the origin / legitimacy of digital media, can also be combined with law for enforcement.
2. **Awareness and Education:** Better awareness of the risk posed by deepfakes, and information regarding provisions of DPDP Act etc, will empower citizens to make more informed decisions over their data and its usage or misuse
3. **International Cooperation:** As the internet is a global tool, some level of international cooperation will need to be undertaken for tackling the cross-border implications of

²² Digital Personal Data Protection Act, 2023, No. 22 of 2023, § 6 (India).

²³ Digital Personal Data Protection Act, 2023, No. 22 of 2023, § 12 (India).

deepfake technology²⁴.

ROLE OF REGULATORY BODIES

ADVISORIES TO INTERMEDIARIES

On December 27, 2023, MeitY exercised its authority under Rule 3(1)(b) of the IT Intermediary Guidelines to ask Meta and Google to supervise and regulate false information and deep fakes. MeitY directed Generative AI content to have identifiable metadata or digital marks as of 01 March 2024²⁵.

LEGAL INSTRUMENTS USED

Intermediaries may incur legal liability under the IT Act of 2000 and IT Guidelines (Intermediaries) Rules 2021) such as a 3-year prison term and 71 lakh rupees fine for failing to remove an impersonation deep fake or manipulated media within 24 hours. The IT Act of 2000, section 66D, speaks of impersonation through a device²⁶.

BROADER AI GOVERNANCE

MeitY participates in the India AI Safety Institute (launched in January 2025) to assist in the formulation of ethical and safe standards for AI. In collaboration with UNESCO, she has worked on AI readiness and ethical guides for the safe use of AI in India²⁷.

CONSTITUTION OF INDIA

The Constitution of India acknowledges certain basic rights that all Indian citizens enjoy, which are very important to shield them from threats such as deepfakes. The right to life Article 21 of the Constitution of India ensures the right to a fair trial. The Supreme Court of India has defined this right in wide art concept, which not only consists the dignity and privacy but also includes the reputation of a person as well. In the context of deepfakes, particularly sexual deepfakes, making or sharing such content without consent violates a person's dignity, privacy and bodily autonomy. It follows that victims can assert the breach of their fundamental right to live with

²⁴ Preksha Singh, *Deepfakes, Identity Theft and the Dark Web: Legal Gaps in AI-Generated Fraud – An Indian Perspective*, *Int'l J. Civ. L. & Legal Rsch.* (2025).

²⁵ Ministry of Electronics & Information Technology, *Advisory on Deepfakes and Metadata Requirements* (Gov't of India, New Delhi).

²⁶ Ministry of Electronics & Information Technology, *AI Content Advisory with Watermarking Requirement* (Gov't of India, New Delhi).

²⁷ Ministry of Electronics & Information Technology, *AI Safety Institute Launch Press Release* (Gov't of India), <https://www.meity.gov.in>.

dignity under Article 21 when deepfake pornography is made and circulated. Fundamental rights under the Indian Constitution also play significant role in protecting individuals from such harms including use of deepfakes. The Constitution of India ensures the right to life and personal liberty under Article 21. In the context of deepfakes particularly sexual deepfakes producing or distributing such content without consent is a breach on a person's dignity, privacy and bodily autonomy. Article 21 gives victims a legitimate claim against deepfake pornography, as it violates their right to live with dignity.

In India, Article 19(1)(a) of the Indian Constitution of India provides citizens the right to freedom of speech and expression. This right enables individuals to express their opinions, exchange information, and communicate openly, including through digital platforms. However, this freedom is not unlimited. Under Article 19(2) of the Constitution of India, the State is permitted to apply reasonable limitations in the interests of public order, decency, morality, defamation, and the security of the State. Therefore, the creation or distribution of harmful deepfake content particularly material that is defamatory or sexually explicit cannot be justified as free speech. Such acts infringe the dignity, privacy, and rights of individuals and do not receive the protection of constitutional freedom of expression²⁸.

Justice K.S. Puttaswamy v. Union of India

The Supreme Court decision that recognizes privacy as a fundamental right under 14, 19, and 21 is historic and while it does not deal with deepfakes directly, it is an excuse for more lawsuits in the AI/digital sphere. It is about to become more difficult to legally justify digital manipulation²⁹.

RECOMMENDATIONS

1. Standalone Deepfake Regulation Acts should be enacted. Each Act should include definitions of "deepfake" and "synthetic media" and which include provisions and penalties for malicious creation and distribution of these media without the consent of the individuals involved.
2. Amendments to the Information Technology Act, 2000 should be made, or deepfake provisions incorporated into the Digital India Bill (if applicable) for the expansion of

²⁸ INDIA CONST. art. 21; INDIA CONST. art. 19(1)(a), (2).

²⁹ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India).

- the provisions of Sections 66C, 66E, and 67A to include AI impersonation.
3. Bring to the attention of the judiciary the violation of individuals and their Digital Personality Rights, including the violation of their right to be portrayed, heard, and identified without their consent, as a violation of Article 21 of the Constitution of India.
 4. Call for the inclusion of watermarks and other metadata pertaining to the creator of AI-generated products.
 5. Amendments to the intermediary provisions of the law should be made to establish a duty to eliminate illegal deepfake materials within 24 hours upon a complaint and to provide a duty to the intermediary to produce a transparency report.
 6. A Deepfake Regulatory Task Force should be created within the Ministry of Electronics and Information Technology or Indian Computer Emergency Response Team to deal with Deepfake related allegations and autonomous complaints. During election times, the Election Commission of India should be empowered to issue immediate Deepfake complaints.
 7. Ensure that the government detection mechanisms that are used are in compliance with the legal, necessities, and proportionality requirements of the law as established in Justice K. S. Puttaswamy (Retd.) v. Union of India.
 8. Public Education and Digital Literacy \Launch organized, nationwide campaigns on media literacy and educate citizens to identify and report deepfakes.

CONCLUSION

The rapid development of Artificial Intelligence has caused deep fake technology to become more easily obtainable and has created the potential for many dangers regarding privacy, consent, and dignity, especially when sexually illicit, or non-consensual materials are produced without someone's knowledge. Such a misuse has a potential to ruin a person's reputation and wellbeing, violating their constitutional rights to privacy and dignity. The Indian constitution has some legal remedies to this problem in the Bharatiya Nyaya Sanhita, 2023, The Information Technology Act, 2000, and the Digital Personal Data Protection Act, 2023. Each of these provide legal remedies to issues of defamation, impersonation, cybercrimes, and misuse of personal data. Nevertheless, these laws tend to only indirectly regulate the issues regarding deep fakes and give few to no definitions, causing a wide variety of enforcement issues such as anonymity, encrypted communications, and a lack of digital forensics. For this reason, a more comprehensive legal framework is necessary in order to achieve a clear definition of deep fakes as well as strengthen accountability of digital platforms by instituting procedural

safeguards such as a digital watermark. This would create a better system that rule societies as well as preserve the dignity and privacy of individuals within a society.

REFERENCE

1. Statutes and Legal Instruments:

- The Constitution of India, 1950.
- The Information Technology Act, No. 21 of 2000, India Code (2000).
- The Bharatiya Nyaya Sanhita, No. 45 of 2023, India Code (2023).
- The Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).

2. Journal Articles:

- Preksha Singh, *Deepfakes, Identity Theft and the Dark Web: Legal Gaps in AI-Generated Fraud – An Indian Perspective*, Int'l J. Civ. L. & Legal Rsch. (2025).
- Danielle K. Citron & Robert Chesney, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 Calif. L. Rev. 1753 (2019).
- Bobby Chesney & Danielle Keats Citron, *Deep Fakes and the New Disinformation War*, Foreign Affairs (2019).

3. Cases:

- *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India).
- *R. Rajagopal v. State of Tamil Nadu*, (1994) 6 S.C.C. 632 (India).
- *State of Maharashtra v. Mohd. Yakub*, (1980) 3 S.C.C. 57 (India).