SUPREMO AMICUS

INDIA'S FIRST AI INTEGRATED LAW JOURNAL

Peer Reviewed, Refereed and Open access Journal

- Available in 331+ International Libraries
- Indexed at 32 Databases

ISSN NO. 2456-9704
Volume 10 Issue 1
www.supremoamicus.org

DISCLAIMER

The information presented in this article is intended for general informational and educational purposes only. While every effort has been made to ensure that the content is accurate, up-to-date, and reliable at the time of publication, the editorial board and publisher make no representations or warranties of any kind, express or implied, regarding the completeness, accuracy, reliability, suitability, or availability of the information contained herein.

The views and opinions expressed in this article are those of the author and are based on personal research, experience, and interpretation. They do not necessarily reflect the official policy, position, or opinions of any affiliated organization, institution, or entity.

This article is not intended to serve as professional advice of any kind. The editorial board and publisher shall not be held liable for any errors or omissions in the content, nor for any losses, injuries, or damages arising from the use of or reliance on this information.

ABOUT THE JOURNAL

Supremo Amicus is an online, peer-reviewed international journal devoted to the interdisciplinary fields of law and science. In an era marked by rapid technological progress and evolving legal frameworks, the journal seeks to bridge the gap between these two dynamic domains by offering comprehensive and critical insights into their various aspects. The journal places a strong emphasis on contemporary advancements, emerging trends, and the complex challenges faced by both the legal community.

The primary objective of the journal is to encourage and promote original, high-quality research. It is committed to publishing well-researched, analytically sound, and thought-provoking articles that adhere to rigorous academic standards. Each submission undergoes a thorough peer-review process to ensure authenticity, relevance, and scholarly integrity. In doing so, the journal maintains its commitment to excellence and credibility.

In addition to fostering research, the journal aims to make complex ideas accessible and engaging for a diverse readership. It strives to present content that is not only intellectually enriching but also clearly written and reader friendly.

Furthermore, the journal is committed to promoting interdisciplinary collaboration and global engagement. It welcomes diverse perspectives from contributors across different regions and backgrounds, thereby enriching the quality and scope of discussions presented within its pages.

With this vision we proudly present Supremo Amicus to our readers.

-Editorial Team
Supremo Amicus

CRIMINALIZATION OF NON-CONSENSUAL DEEP FAKE PORNOGRAPHY IN INDIA: CRITICAL LEGAL ANALYSIS AND THE NEED FOR AN EXTENSIVE STATUTORY REFORM

By *Gauri Pandey*
From *Amity Law School, Noida,* **Amity University, Uttar Pradesh**

Abstract

The rapid development of Artificial Intelligence (AI) has led to the development of deep fake technology, which has become a powerful medium for digital exploitation in today's era of synthetic media. Non-Consensual Deepfake Pornography (NCDP) is the most widespread and harmful use of this deep fake technology, which is made through the use of AI. This paper explores the significant legal concerns raised by this image-based sexual abuse. It argues that the nuances of AI-generated harms, which go beyond the conventional definitions of obscenity, defamation, or voyeurism, cannot be adequately addressed by India's current legal framework. This study creates a conceptual framework that characterizes deep fakes as a digital infringement on human dignity and bodily autonomy rather than just false information. Through a critical analysis of the existing Indian legal system, this study finds a notable legislative lag. The core of synthetic violation, in which harm is caused from the illegal replication of an individual's likeness in a sexual context, is not adequately captured by the present laws. Victims frequently lack a clear route to justice as the result of these interpretive obstacles and factual complexity. This paper further presents a comparative examination of international legal remedies to fill up these gaps, looking at how the countries like The United States of America, South Korea, the United Kingdom, China, and the European Union, Japan, Australia have progressed towards this problem and how India can use these precedents as a guide to move from a patchwork legal system to a specific statutory structure. The structural drawbacks in the present structure are explained along with the suggestions and recommendations. In the end, this dissertation argues that in the absence of significant statutory reform, digital dignity of people is still in jeopardy, which requires a legal framework that is as advanced in technology as the instruments that it aims to control.

Key Words: Non- Consensual Deepfake Pornography (NCDP), Deepfake, Artificial Intelligence (AI), Technology, Legal framework, Indian Statutes, Statutory Reform, Criminalise, Amendment, New Statute, Digital, Law

Chapter 1: Introduction

A post-truth era has emerged as the result of artificial intelligence's quick development, when the lines separating the real-world reality from digital world are becoming increasingly blurred. The production of Deep fakes, hyper-realistic digital alterations of photos, movies, or audio recordings, is one of the most malicious uses of generative AI. Even if technology has enormous potential for the entertainment and education industries, its weaponization in the pattern of Non-Consensual Deep fake Pornography is a grave breach of people's privacy, dignity, and physical autonomy. The spread of NCDP in India is a growing issue of privacy as well as a technological problem. It entails putting an individual's image into sexually explicit content without that person's consent using deep-learning algorithms, particularly Generative Adversarial Networks. Deep fakes cause irreversible reputational harm, psychological pain, and social exclusion because, in contrast to typical photo alteration, their seamless appearance renders them unrecognisable from reality to the unaided eye. The present Information Technology Act, 2000, the primary statute related to digital laws and cyber-crimes was created for a pre-generative AI environment, which makes this study crucial given the current legislative void. This dissertation promotes a comprehensive legislative change that acknowledges NCDP as a unique criminal offense based on a

violation of digital personhood, arguing that the existing gradual approach is inadequate.[1]

Chapter 2, which defines the mechanics of the deep fake technology and unique characteristics of NCDP lays the intellectual understanding of the study and starts the foundational discourse of this research. This examines how do the words deep learning and fake are combined together to develop the content that closely matches real people to the extent that it can trick viewers into believing that those things happened in reality. This chapter makes a difference between NCDP and traditional image-based abuse. Unlike the traditional image based abuse, that mostly depends on the unlawful sharing of an actual intimate images, NCDP is often completely synthetic, artificial, creating a special legal challenge when the harm results from the unlawful sexualization of a person's identity rather than the recording of a physical act. This chapter describes NCDP as a serious violation of a person's right to self-determination and the control over one's own portrayal in the real and virtual world. Chapter 2 shows that NCDP presently occupies an ambiguous legal domain that requires a precise, contemporary definition to ensure legal certainty and effective deterrence by pointing out the shortcomings of the present laws like the IT Act, which were not drafted with the AI-generated crimes in mind.[2]

Building on this framework, the next chapter offers us a detailed and critical analysis of India's present legal system. This chapter studies the Information Technology Act, 2000, with a particular focus on Sections 66E, 67, and 67A, that addresses the disseminating pornographic content and privacy concerns.[3] Additionally, the chapter examines and understands the Digital Personal Data Protection Act, (DPDP) 2023, evaluating if the right to be forgotten can successfully stop NCDP from spreading or not.[4]

Understanding that the digital sphere is worldwide, Chapter 4 presents a foreign comparative analysis of the countries that have already made laws on NCDP. The innovative laws of South Korea that have specifically forbidden the production and dissemination of deep fakes with malicious intent are studied. The Online Safety Act, which focuses on both the platforms hosting the content and the offenders, is used to assess the strategy of United Kingdom.[5] While the United States is studied for its combination of federal initiatives and the state-level right of the publicity laws, the European Union continues to focus on the AI Act, which imposes stringent transparency and labelling standards.[6]

The study's reformative core is found in Chapter 5, which reflects the drawbacks of the present legal system, talks about the Deep fakes Regulations of 2025, and provides recommendations for the future. Finally, the study's conclusions are summarized and a strategic road map for the stakeholders is provided. It reaffirms that India's current legal system is a patchwork quilt which exposes people to high-tech abuse. This last chapter urges lawmakers to approve a proposed definition of the synthetic non-consensual sexual material and demands that enforcement agencies receive specialized training to differentiate between actual and deep fake media. It also highlights digital platforms' obligations with relation to the watermarking and the metadata transparency. In the

[1] Data Secure India. (n.d.). Deepfake technology in India: Legal framework for misinformation and image rights.
[2] Bhattacharjee, R., & Sharma, M. (2025). Deepfake & pornography: The coming crisis of privacy and consent. South Eastern European Journal of Public Health, XXVI(S2), 1196–1213.
[3] India. (2000). The Information Technology Act, 2000 (Act No. 21 of 2000, updated version). Government of India
[4] Ministry of Electronics and Information Technology, Government of India. (n.d.). Digital Personal Data Protection Act, 2023.
[5] UK Parliament. (2023). Online Safety Act 2023 (c. 50). legislation.gov.uk.
[6] European Union. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). EUR-Lex.

end, the dissertation concludes that even though technology will always surpass law, the legal authority must work to keep pace to safeguard citizens' fundamental rights in a society that is becoming increasingly digitalized daily.

1.1 Statement of the Research Problem

The rapid proliferation of artificial intelligence has ushered in an era of unprecedented digital innovation, however, it has also given rise to numerous negative issues, particularly with regard to non-consensual deepfake pornography. Deepfakes, artificial media created by machine learning algorithms that impose a person's likeness in an explicit content without that person's consent, are the new forms of sexual assault. Unlike traditional revenge porn, which relies on real images or recordings, NCDP produces hyper-realistic obscene content from publicly available photos, often from social media. This technology causes serious psychological, emotional, and reputational harm to victims while evading present legal structures designed for real imagery. This innovation is difficult for India's legal system because it is built on pre-Artificial Intelligence legislation. Since deepfakes and synthetic sexual imagery are not legally defined, their creation, ownership, and distribution are left unregulated. All these problems gives the main research statement for this study: Why do India's present legal measures fail to sufficiently regulate and punish the non-consensual deep fake pornography, and what laws and policies should India adopt? This calls for a careful analysis of definitional gaps, enforcement challenges, remedial shortcomings, and the under-criminalization of synthetic activities. It looks at the comparative effectiveness and the constitutional balances without totally rewriting the current structures and offers solutions including victim-centric procedures, platform commitments, graded sanctions, and explicit definitions. Because AI is democratizing harm while the current rules are only stagnating, the current research challenge is crucial and highly required. For the sake of justice, prevention, and India's position as a worldwide leader in the digital sphere, it is imperative that this issue be addressed through comprehensive law reform.

1.2 Research Objectives

The purpose of this dissertation is to critically examine the necessity for India's legal system to make non-consensual deepfake pornography illegal, highlighting shortcomings in the existing legislation and proposing comprehensive legislative reform. The primary topic of this study is how deepfake technology has evolved into a tool for grave violations of the autonomy and dignity of an individual, particularly when it comes to the unapproved creation and dissemination of false intimate photos. The objective is to assess whether the current legal frameworks adequately handle the unique features of this damage, such as its scalability, easy accessibility, and dishonest nature, and to advocate for a particular legislation that recognizes it as a distinct breach. This analysis begins with a conceptual characterization of deepfakes and their non-consensual expressions in order to offer a theoretical basis for additional research. Further, it evaluates how well the existing domestic legal rules regarding privacy, reputational damage, and digital misconduct can be interpreted to address the development, spread, and use of deepfakes. Comparing India's approach to international models that have established explicit bans, enhanced platform liability, and the victim compensation procedures is a very important objective. This dissertation combines doctrinal analysis, comparative insights, and impact-oriented reasoning in an effort to offer a scholarly momentum towards a strong legal architecture.

1.3 Research methodology

This dissertation is based on the doctrinal research approach, which is standard in legal studies. Doctrinal research involves carefully analyzing and assessing laws, judicial decisions, and significant texts to ascertain their efficacy and meaning. Before forming conclusions, it makes use of strategies including accepting laws literally, analyzing their intent, or making sure that a number of elements work together harmoniously. For a problem like outlawing non-consensual deepfake pornography, this strategy is perfect. It is only a question of legal principles, not data or interviews; the task is to assess how well

current laws address this new technological problem and offer suggestions for solutions. Deepfakes challenge established privacy laws in new ways, like by being deceptive or spreading quickly.

Doctrinal analysis enables us to examine the text of law directly in order to find weaknesses, such as the lack of rules regarding artificial intelligence-generated fake images. It also works very well for comparing Indian laws with those of other nations, using simple side-by-side reasoning to identify key ideas. The methodology follows the study's natural flow, outlines the principles, evaluates the state of affairs, looks abroad, takes human costs into account, and plans ahead of time. It is also helpful because it only requires quality books and papers and doesn't require fieldwork. Doctrinal research is excellent at creating convincing arguments from the law itself, even if it overlooks actual numbers. In this instance, it offers a solid basis for promoting real legislative changes in our digital world.

1.4 Literature Review

The growing body of research on deepfakes makes it clear that this is no more just a technological advancement but rather a serious legal problem that sits at the nexus of digital legislation, consent, privacy, and dignity of an individual. At first, deepfakes were often seen as a technological advancement, but the emphasis has gradually shifted to the potential harm they may cause, especially when they are used to create obscene content without consent. This shows that the issue encompasses identity theft and infringement of personal autonomy in addition to fake media. This larger body of studies provides a strong basis for this paper because it confirms that the NCDP should be seen as a legal wrong with real human consequences rather than as a minor internet misuse. It is mostly challenging to penalize the wrong in a legal system that does not clearly define it. This literature talks about this gap. Another important area of research is the speed and persistence of injury. Once this kind of content is created and shared, it may spread swiftly, be copied endlessly, and endure despite attempts to remove it. This suggests that the primary act is not the end of injury. It keeps evolving. A generic or slow reaction is often too late, which poses a special problem for legal institutions. A system that functions quickly, clearly, and decisively is important for the victims.

Therefore, this present writing supports the idea that India needs more specific provisions for this problem. It is very important to have a framework that explicitly addresses the creation, circulation, immediate shutdown, and responsibility of these deep fakes. Another important part of this study is the comparative analysis with the laws of a few global counterparts. These studies are helpful not because they offer pre-made remedies but rather because they show that legal systems can directly handle this problem without compromising free expression or creativity. The primary lesson is very simple that when the harm is clearly defined by the law, it is easier to prevent, control, and punish it. But these similarities also draw attention to an important aspect. No foreign model can be mindlessly copied. India has its own legal system, social reality, and enforcement problems.

Thus, the real question is not only just what others have done, but also what could be successfully adjusted for India. A very less research has been done on non-consensual deepfake pornography as a distinct legal concern. Some discuss legal shortcomings, but they don't inquire as to what kind of legislative or regulatory structure India should actually put in place. Others mention reform in general terms, but they don't explain why the current laws don't sufficiently punish and regulate the behavior. That is the focus of this dissertation. Despite being grounded in recent research, this study goes beyond it by asking a more direct question that what should India do in the end, and why is the existing framework inadequate?

Chapter 2: What is Deep Fake and NCDP?

The creation, distribution, and consumption of digital information have all undergone a significant change because of artificial intelligence. The emergence of deepfake technology, which uses machine learning

algorithms to manipulate a person's likeness to create incredibly realistic synthetic images, audios, and videos, is one of the most significant advancements in this sector. Although, this technology has its valid uses in the accessibility, education, entertainment, and creative media, its abuse and misuse has raised significant ethical and legal questions on its fair use.[7]

Non-consensual deep fake pornography, which is defined as the sexually explicit synthetic content that is made by using a real person's face, resemblance, or identity without the consent of that person, is one of the most serious examples of this misuse.This type of content violates people's autonomy, privacy, and bodily integrity and is misleading also. This problem has grown lately in India because of the rapid development and progress of digital platforms, and this has made it easier, faster, and more challenging to govern the creation and distribution of this content.[8]The terms deep learning and fake are combined together to form the term deep fakes, which shows the technological base of its production.

Technically speaking, deep fake systems are trained on massive datasets of pictures, videos, or voice samples to produce artificial material that closely mimics a real person. Because of this realism, the technology is especially risky in abusive situations because the generated footage may deceive viewers into thinking that someone has engaged in behaviour that never happened. When it comes to pornography, the victim may be shown in explicit sexual acts without ever having taken part in them or given permission for their image to be used in that way.

In addition to the material's untruth, the injury results from the victim's wrongful sexualization and the creation of a permanent digital content that can be shared extensively and perpetually. The conventional kinds of image-based abuse and regular pornography can be distinguished from non-consensual deep fake pornography. In deep fake pornography, an individual's likeness is digitally placed into explicit footage without consent. While a deep fake pornographic act can be completely synthetic and may not contain any original intimate photographs at all, regular image-based sexual abuse frequently uses real intimate images that were shot or disseminated without consent. This gap is very important from a legal point of view because many present laws were not created with the AI-generated crimes and misuse in mind, but rather with the physical activities, real records, and captured photographs in mind. Because of this gap, NCDP occupies an ambiguous legal area in which the activity is acknowledged but not categorized in the present laws.[9] This type of content causes vast and multifaceted damage. Humiliation, anxiety, sadness, terror, reputation harm, social exclusion, and professional harm are all possible outcomes victims have to face. The harm caused by this fake sexual content is irreversible and challenging to remove because it can get replicated, re- posted, and spread across a number of channels. The archived or the re-uploaded copies may still exist even if a platform deletes the original content. If compared to the other types of internet abuse, the non-consensual deep fake pornography is particularly harmful because of its long lasting nature and widespread distribution.[10] At present, the Indian laws offers only scattered and incomplete solutions for this problem. There are two clauses in the Information Technology Act of 2000 that are frequently regarded useful when we discuss the negative effects of deep fakes. Section 66E of the IT Act 2000 protects privacy by making it

[7] Data Secure India. (n.d.). Deepfake technology in India: Legal framework for misinformation and image rights.

[8] Narmadha.L. (2025). An Analysis of Legal Gaps and Enforcement Challenges in Addressing AI-Generated Deepfake Sexual Offences in India. International Journal of Advanced Research in Science, Communication and Technology.

[9] India. (2000). The Information Technology Act, 2000 (Act No. 21 of 2000, updated version). Government of India.

[10] Bhattacharjee, R., & Sharma, M. (2025). Deepfake & pornography: The coming crisis of privacy and consent. South Eastern European Journal of Public Health, XXVI(S2), 1196–1213.

illegal to intentionally take, publish, or transmit photos or videos of someone's private area without that person's consent. Similarly, the publication or transmission of pornographic content in electronic format is prohibited under Section 67 of the IT Act. These provisions are important because they show us that the obscenity and invasions of privacy are already considered as crimes under the Indian law.

However, these laws do not specifically mention about deep fake pornography, and the AI made content. This raises a lot of concern about whether and how these laws apply in the situations where the content is created and not documented.[11]For instance, any fake intimate image made through AI is not easily covered by Section 66E, and it only includes the misuse of real private photos. The particular harm related with the non-consensual deep fake pornography cannot be captured by obscenity alone, despite of Section 67 provision on the obscene digital media. In these situations, the primary harm is not obscenity in the conventional sense, but rather the unapproved sexualization of an individual's identity. As a result, depending only on these clauses compels investigators, prosecutors, and judges to interpret statute language in ways that go beyond its intended meaning. Both the victims and the authorities experience less legal certainty as a result of inconsistent enforcement. The lack of a precise legal definition of deep fakes or synthetic pornography in the Indian law is another indication of the shortcomings of the current legal system. The legal system lacks a solid foundation for defining the behaviour, categorizing the offense, and creating appropriate remedies in the absence of such a description. In reality, victims frequently have to rely on a hodgepodge of laws under criminal law, cyber law, and the privacy principles, none of these adequately addresses the production, ownership, distribution, or threat of distribution of non-consensual deep fake pornography. Victims bear a significant burden as a result of this disjointed strategy, as they must demonstrate harm through an indirect and frequently insufficient legal channels. Additionally, because criminals can take advantage of uncertainty and enforcement weaknesses, deterrence is weakened.[12]

This problem requires a grasp of the conceptual relevance of consent. Non-consensual deep fake pornography is essentially an offense against the victim's autonomy since it violates their right to control how they are portrayed and whether or not their image is utilized in private settings by using their likeness in sexual content without their consent. Consent is very important in both the real and virtual worlds. Mostly. The synthetic media turns identity of a human into a mere tool of exploitation. Thus, deep fake pornography should be seen as a serious kind of sexual violation that harms human security, privacy, and dignity. A wider doctrinal stance in India demonstrates that while privacy and cyber law have developed, but they have not yet completely adjusted to the difficulties presented by generative AI. The structure of the Information Technology Act, 2000 reflects a pre-AI notion of digital harm because it was passed long before the deep fake technology became generally available. The lack of a specific legal framework implies that enforcement is reactive, inconsistent, and depending on the specific facts of each case, even though existing regulations may be used in some situations. Because of this, the legal reaction is susceptible to delay and ambiguity in interpretation, particularly when it comes to content that is stored on any foreign platforms, and shared anonymously, or produced using quickly developing AI techniques.[13]As a result, non-consensual deep fake pornography should be considered a separate type of digital sexual assault that falls somewhere between gender justice, privacy law, obscenity law, and cyber

[11] India. (2000). The Information Technology Act, 2000 (Act No. 21 of 2000, updated version). Government of India\

[12] (2025). Deepfake technology and its legal implications in India. International Journal of Advanced Research in Science, Communication and Technology, Paper No. 27634.

[13] Data Secure India. (n.d.). Deepfake technology in India: Legal framework for misinformation and image rights.

crime. Its detrimental effects go far beyond reputation injury to include the psychological trauma, identity theft, coercion, and the long-term social impact, and it is not sufficiently covered by current legal measures. Thus, this chapter's conceptual framework demonstrates that the issue is both technologically innovative and legally under-addressed. This conclusion goes straight to the following chapter, which will take a close look at the current Indian legal system and evaluate the extent to which the offense of non-consensual deep fake pornography can be addressed by existing statute provisions, interpretations of the judiciary, and enforcement procedures.

Chapter 3- Current Indian Statute for NCDP

The NCDP is a major example of how quickly a developing technology can worsen an already severe injury to something far more invasive, and impossible to reverse. The spread of the pornographic or explicit content is not the only problem. On a more deeper level, it symbolizes the theft and manipulation of an person's identity, a serious violation of their secrecy, and the burden of a sexual description on a person who neither contribute or approved of its production or distribution. As a result of this, the damage is not just on the reputation. It becomes personal, psychological, and long-lasting in nature. Presently, the Indian law has not created a single, comprehensive, and unambiguous law that specifically covers this type of abuse. Although some protection is provided through some of the laws, but they were intended to address the crimes done by using AI.

Let us look at the present legal provisions in this matter. The deep fake-related crimes in India, particularly the ones that are done using computers, are covered by the Information Technology Act of 2000. Section 66D of the Act particularly addresses those situations in which a computer or any other communication device is used wrongfully for the purpose of identity theft and fraud. This section focuses on the circumstances in which people are forced by the technology to speak or do things that lead to cheating. The use of deep fakes for privacy violations is covered under Section 66E of the Information Technology Act 2000. This section explains about the invasion of privacy that happens when someone's private photos or videos are obtained, shared, and published using deep fakes without the consent of that person.[14]

Further, the deep fakes with an explicit or pornographic content are subjected to Section 67A and section 66B of the Information Technology Act, 2000. These sections provide the fines and punishments for the publishing and distributing of graphic and obscene content involving adults and children. The intermediaries, or the websites where the deep fake content is posted, are liable under Section 79 of the Information Technology Act 2000. This provision requires the intermediaries to remove any explicit content either upon receiving a court order or upon becoming aware of its existence. In the Myspace Inc. v. Super Cassettes Industries Ltd. ruling, the court emphasized that intermediaries must remove infringing content as soon as private parties warn them of copyright infringement, even in the absence of a court order.[15]

Important offenses include voyeurism, defamation, impersonation, obscenity, and the digital distribution of pornographic material. Obscenity related offenses frequently place more emphasis on upholding social standards than on consent issues or identity misuse. The basis of defamation law is whether someone's reputation was damaged. Additionally, voyeurism implies that someone was observed. However, because these provisions were not created with fake sexual content in mind, they only offer a few limited forms of recourse.As a result, when they are applied to deep fake misconduct, they usually provide very

[14] India. (2000). Information Technology Act, 2000 (Act No. 21 of 2000). Government of India.

[15] Bhattacharjee, R. R., & Sharma, M. M. (2025). Deepfake & pornography: The coming crisis of privacy and consent. South Eastern European Journal of Public Health, 26(S2), 1196–1213.

little and indirect compensation. The use of authority is restricted to particular action by this variety of clauses.[16]

Social Media Intermediaries (SSMIs) became subject to new rules in 2021 when the Information Technology Rules were introduced. Intermediaries with more than a certain number of the registered users must designate staff members to keep an eye on and identify the source of information and particular sorts of material in order to qualify as SSMIs. The regulations include a grievance settlement procedure for intermediaries to handle user complaints and grievances, and they ensure a more reliable framework for handling content-related concerns. The rapid development of machine learning and artificial intelligence technology has led to the emergence of deep fakes of pornography. Deep fake technology has deep roots in India, particularly given its widespread application in situations of revenge defamation, politics, pornography, and the film industry. The Justice K.S. Puttuswamy (Retd.) and another vs Union of India Case claims that it infringes upon the fundamental right to "privacy" protected by Article 21 of the Constitution of India.[17]

India's recognition of privacy as a basic right has gradually changed as a result of many judicial interpretations. In early cases such as M.P. Sharma v. Satish Chandra (1954) and the Kharak Singh v. State of Uttar Pradesh (1962), a narrow meaning of privacy was acknowledged. In the M.P. Sharma v. Satish Chandra (AIR 1954 SC 300) case, the Supreme Court curtailed the right to privacy with relation to search and seizure by holding that it was not specifically protected by the Constitution. Similarly, the Court acknowledged some aspects of the right to personal liberty under Article 21, particularly with regard to police visits to homes, but rejected privacy as a distinct right in the Kharak Singh case. These cases shows a narrow reading that put the state's interests.

The landmark case of Justice K.S. Puttaswamy lead to a reform. The earlier decisions were overturned unanimously by the nine- judge panel through acknowledging privacy as a very crucial element of the right to life and personal liberty under Article 21 of the constitution. The court laid a strong constitutional foundation by emphasizing privacy as essential to human dignity, uniqueness, and liberty.

This decision emphasized several key concepts affecting the privacy rights in this digital age. It recognized the basic component of informational privacy, which comprises an individual's sovereign right over their personal data. The court emphasized consent as a prerequisite for data collection in order to safeguard autonomy of people over their information.
The landmark case of Justice K.S. Puttaswamy lead to a reform. The earlier decisions were overturned unanimously by the nine- judge panel through acknowledging privacy as a very crucial element of the right to life and personal liberty under Article 21 of the constitution. The court laid a strong constitutional foundation by emphasizing privacy as essential to human dignity, uniqueness, and liberty. This decision emphasized several key concepts affecting the privacy rights in this digital age. It recognized the basic component of informational privacy, which comprises an individual's sovereign right over their personal data. The court emphasized consent as a prerequisite for data collection in order to safeguard autonomy of people over their information.The one limitation that was highlighted was the need that data should be utilized only for specified purposes.[18]

[16] Patil, S. S., & Mishra, S. P. (2026, February 17). Deepfake pornography and criminal law of India: The crises of legal classification. Indian Journal of Law and Legal Research.

[17] Bhattacharjee, R. R., & Sharma, M. M. (2025). Deepfake & pornography: The coming crisis of privacy and consent. South Eastern European Journal of Public Health, 26(S2), 1196–1213.

[18] Kumar, D. (2025). The right to privacy under Article 21: Implications of the DPDP Act, 2023 for data protection in India. International Journal of Legal Research Publication.

Additionally, the concept of proportionality was developed, which requires that any state invasion of the private property should be justified, proportionate, and thoroughly investigated. These concepts have important implications for data security, particularly in terms of addressing problems caused by digital technologies. This decision, which emphasized the need for a comprehensive data protection framework to safeguard privacy against unauthorized data collection, surveillance, and breaches, also led to the formation of the Digital Personal Data Protection (DPDP) Act of 2023 and other legislative amendments.[19]

India did not have a comprehensive data protection provision before the introduction of the DPDP Act of 2023. The Information Technology Act (IT Act) of 2000 was therefore in charge for the data protection. The DPDP Act defines data as a representation of information, knowledge, facts, concepts, or instructions that are being prepared or have been prepared in a formalized manner, are intended for processing, are being processed, or have been processed in a computer system or computer network, and can take any form, such as the computer printouts, a magnetic or optical storage media, punched cards, or punched tapes, and stored internally in the computer memory. Similar to the GDPR, the DPDP Act covers the digital personal data, although it is more restrictive and excludes organizations outside of India that keep an eye on the actions of Data Principals. Additionally, the DPDP Act sets rights for the people whose data is gathered and utilized, establishes the purpose limitation obligations, and imposes strictly specified requirements for processing digital personal data. Additionally, it creates the Data Protection Board (DPB), a regulatory body that looks into complaints and imposes fines but is not able to make rules or recommendations. The DPDP law is a revolutionary law that expands the use of the personal data processing to every organization, regardless of their size or private status. It took inspiration from the General Data Protection Regulation (GDPR) of the European Union. Additionally, if the procession of digital personal data is connected to any action relating to the offering of products or services to the Data Principle within the Indian territory, it has considerable extraterritorial application. However, there was no mention of behaviour monitoring in the final text of the law, so it's still not clear if this would also involve it. A household exemption is also included in Section 3(c) of the DPDP Act where data processing is done exclusively for domestic or personal purposes. Similarly, the Act does not apply to personal data that is made available to the public by the data subject or by the law. In other words, regardless of whether the goal for which this was gathered has been fulfilled, the government may keep personal information for an indefinite amount of time. People's fundamental rights to information and privacy, which are derived from the Constitution, must be protected and balanced by a data protection law.[20] As a result, the DPDP Act has been insufficient to adequately safeguard personal information in the digital age. Additionally, it cannot defend women's dignity because it cannot safeguard personal information, which might lead to a surge in numerous cyber crimes against women, such as deep fake videos and cyber pornography.

The DPDPA makes no mention of the Data Fiduciary's obligations with regard to AI-generated media. However, the obligation stated in Section 8(5) might be expanded to ensure that any illegal content created with data that a Data Fiduciary has access to be removed as soon as it is found. Even if it is anticipated that the data shall be used to make a decision which affects the Data Principal, a Data Fiduciary is required by Section 8(3) to ensure the accuracy and completeness of the data. The term probably expands the range of Data Fiduciaries' responsibilities to take deep fakes into account, including social media companies. It should be mentioned that the foundation of Data Fiduciaries' business model is the use of users'

[19] Ibid.

[20] Bhattacharjee, R. R., & Sharma, M. M. (2025). Deepfake & pornography: The coming crisis of privacy and consent. South Eastern European Journal of Public Health, 26(S2), 1196–1213.

personal information for targeting ads and present them with material that is relevant to their interests. As previously said, even deep fake itself may be regarded as personal information that can be utilized to identify and determine actions that impact the Data Principal. This can be approached in two different ways. First, by using deep fake as one of the input data points for its algorithm, Data Fiduciary can show targeted content to the person it features. Second, a user who already consumes or is probably to consume the content of the person displayed there may be recommended a deep fake. To put it simply, the DPDP Act is concerned with protecting an individual's personal information from abuse by "Data Fiduciaries." According to the Act, the Data Fiduciary is any individual who chooses how and why to utilize a person's personal information. A person whose data is collected by a Data Fiduciary is known as a Data Principal.[21] The terms personal data and personal data breach are two more crucial meanings under the Act. According to the act, personal data is any relevant information about an individual that can be used to recognise them. The definition's scope is greatly expanded by the addition of the term any piece of data.

The concept of any information under the European Union Data Protection Laws' definition of personal data might be used as a model for this interpretation. The meaning of this word and, to a large extent, the entire framework of the Act are linked to the obligation of the Data Fiduciary. Section 4 states that a Data Fiduciary may only utilise personal data for purposes for which the Data Principal has granted explicit consent. Furthermore, as stated in section 7, a Data Fiduciary may use personal data for other acceptable purposes. They generally include abiding by any decision or legal requirement. This guarantees that a Data Fiduciary will not lawfully gather an individual's personal data without that person's express consent and use it to train any generative AI models. Because the majority of social media platforms and search engines have a reach to an astounding quantity of personal data, this strategy might be effective. In accordance with this provision, Data Fiduciaries should be obligated to ensure that false content produced by AI is removed from their platforms. These rules ought to mandate that Data Fiduciaries implement methods for recognizing and detecting deep fakes, as this has been a major issue.[22] The current best practices leverage the existing signatures that are unique to each piece of content to identify any potentially tampered-with content. However, current methods fall short in detecting deep fakes.

3.1 The Right to be Forgotten

The Data Principal's right to be forgotten under section 12 of the DPDPA provides additional justification for the Data Fiduciary's removal action. The General Data Protection Regulation also makes reference to this right in Article 17(2). The freedom of speech must be balanced with this right. The public's right to know such information should be balanced with the sensitivity of the personal data, according to Mario Costeja Gonzalez in the European case of Google Sapin SL Google Inc., v. AEPD. Evaluating the extent to which it affects a Data Principal's longivity is also essential. Because a deep fake essentially disseminates inaccurate information about the subject, it has a considerably more detrimental impact on that person. Indian courts have recognized the right to be forgotten as an essential part of the right to privacy protected by Article 21 of the Constitution of India. Quintillion Business Media Pvt. Ltd. v. Zulfiqar Ahman Khan (2019) A Delhi High Court single-judge bench ruled that the right to be forgotten and the right to be left alone are fundamental components of the right to privacy. Additionally, it was noted in the Mahendra Kumar Jain v. State of West Bengal (2021) case that Section 8(1)(j) of the Right to Information (RTI) Act reinforces the protection afforded to an individual's reputation and dignity under Article 21 by upholding their right to privacy. The Section states that certain information is considered personal in

[21] Bhattacharjee, R. R., & Sharma, M. M. (2025). Deepfake & pornography: The coming crisis of privacy and consent. South Eastern European Journal of Public Health, 26(S2), 1196–1213.

[22] Ibid

nature and cannot be published since it would not serve the public interest. Given this, a Data Fiduciary must help a person exercise their right to be forgotten in connection with a deep fake. However, it seems that the DPDP Act does not adequately address the problem of fake generative AI-based media. In this case, the Act's Section 3(c), which describes the situations in which the Act will not apply, is relevant. The first clause states that the Act does not apply when someone handles the data for any domestic or private purpose. It is unclear from the Act what is meant by personal or domestic. It also raises the question of whether someone who illegally obtains another person's personal information can be considered a Data Fiduciary in the Act. Even if the answer is true, fake material produced by artificial intelligence and used for domestic sharing might easily spiral out of hand. This is because, in the age of social media, a deep fake might propagate throughout an ever-widening social circle. It would be quite impossible for the developer to keep track of where their deep fake is heading once it was shared with anyone in their social network or family. Additionally, it should be noted that the DPDP Act does not differentiate between personal and sensitive data. Since there is no such distinction, this confidential personal data is not provided with an additional layer of adequate security. Even if a Data Principal's personal information can be used to identify them, sensitive intimate data includes the information that could be used to discriminate against them. This includes information about their ethnic background, sexual orientation, medical history, and political beliefs.[23] Article 9 of the GDPR permits access to such confidential data under very specific circumstances. More worse consequences, including systematic discrimination or influencing political opinion, could result from a deep fake made using personal data. The current study looks at the protection of both of these data types together as well as the deep fakes that are created from them because the DPDPA does not make this distinction.

By strengthening safeguards against the exploitation of data for deep fake production, the DPDP Rules, 2025 expand on the DPDP Act, 2023 by improving personal data protection measures. The rule 3 highlights the importance of the informed permission and ensures transparency by requiring that notices to the data principals provide explicit information about the acquisition of personal data and its intended uses. Further, to prevent the unwanted access to personal data, that is frequently used to create deep fakes, Rule 6 mandates adequate security measures including encryption and masking. Further, Rule 7 establishes the stringent deadlines for the reporting breaches involving personal data. The data fiduciaries are bound to inform the Data Protection Board and the impacted parties of any breaches immediately. A detailed report should be submitted within 72 hours. This guarantees the prompt action and lowers the possibility that the private information can be exploited to create deep fakes. Also, in order to fasten and manage the process of getting, managing, and withdrawing the user consent, Rule 4 also establishes the Consent Managers, the intermediaries that are registered with the DPB. Together, these steps are reduce the possibility of any kind of data exploitation and improve the data handling effectively. However, there are some loopholes in these regulations.For instance, the regulation of the deep fakes and the synthetic media is ambiguous because of the lack of precise definitions or laws. In order to protect the viewers from any kind of fraud or deception that is based on deep fakes, these regulations do not mandate any content authenticity standards, such as methods to recognize or label the concerned content. Rule 12 highlights the importance of algorithmic audits for the big data fiduciaries even if it lacks specific requirements to regulate AI models that are used to create deep fakes. Additionally, even if the penalties are imposed for data breaches, it is still not clear that who is in charge of the actively creating and spreading deep fakes, which makes this misuse possible. Despite the growing importance of such technologies on the

[23] Bhattacharjee, R. R., & Sharma, M. M. (2025). Deepfake & pornography: The coming crisis of privacy and consent. South Eastern European Journal of Public Health, 26(S2), 1196–1213.

digital democracy and trust, there is also a lack of public education on identifying and mitigating deep fakes. A thorough framework for addressing deep fake-related threats would be provided by filling up these gaps in further modifications or rules.[24]

Because of its overtly sexual content, deep fake pornography is primarily considered obscene material under the Information Technology Act,2000 and the Indian Penal Code (now BNS, 2023). This is seen as such because obscenity laws focus on societal morality rather than the harm caused by unapproved sexual persona alteration. Characterising this as an obscenity issue can divert the discussion away from the victim's autonomy. It will prioritize morality over autonomy and dignity. The judiciary has been moving toward a context-driven approach in recent years, as demonstrated by Aveek Sarkar v. the State of West Bengal 2014.[25] Still, deep fake porn is not well suited to obscenity laws. This strategy is based on the idea that the primary harm caused by deep fake porn is not just the sexual nature of the content but also the lack of permission and identity appropriation. As a result of this, victims suffer a lot, and it becomes difficult for them to seek legal remedy.

People mostly rely on the defamation laws for help because the deep fake pornographic information is sensitive in nature and can seriously damage a person's reputation. The laws related to defamation can turn this crime into a simple loss of a good standing, ignoring the importance of human dignity, morality, and psychological well-being. If deep fake abuse is just conceptualized as reputation harm, it may not be as upsetting to individuals affected. The laws governing these offenses may be appropriate in some situations involving digital sexual assault, but they are insufficient to serve as the main framework for classification. Legal rules pertaining to these offenses were initially intended to target financial schemes rather than considering it as a grave offence requiring serious legal punishment. The Supreme Court's judgement on the prevention secondary harm in a sexual crime proceeding can be more appropriate in those situations when the legal uncertainty and vagueness prolong the victim exposure to these institutional procedures. The case of Nipun Saxena v. Union of India, 2019 provides an evidence for this.

The inaccurate categorization or incorrect classification of any kind often lead to major social and legal repercussions. The affected victims are more likely to experience secondary victimization. The impacted parties eventually lose interest in justice and the criminal justice system as a result. It is caused by protracted procedures, conflicting allegations, and ambiguity over the application of the law. All things considered, deep fake pornography exposes a flaw in the India's penal code with relation to the legal classification of such offenses. Legal remedies will remain disjointed if this behavior is not explicitly recognized by the law as a form of an identity-driven and a sexually motivated harm. Because it interferes with the full protection of affected individuals, this may lead to a reduction in the legal continuity.[26]

3.2 Critical Analysis of the Legal Challenges in India

It is challenging to properly forbid and also enforce the misuse of this rapidly evolving technology due to serious weaknesses and obstacles in India's legal approach to deepfakes.The absence of a clear legal definition of the phrases "deepfakes" and synthetic media in Indian statutes is a significant issue that complicates legal interpretation and responsibility. The current laws like the Information Technology Act of 2000 and the Bharatiya Nyaya Sanhita of 2023, that address similar crimes like identity theft,

[24] Bhattacharjee, R. R., & Sharma, M. M. (2025). Deepfake & pornography: The coming crisis of privacy and consent. South Eastern European Journal of Public Health, 26(S2), 1196–1213.
[25] Patil, S. S., & Mishra, S. P. (2026, February 17). Deepfake pornography and criminal law of India: The crises of legal classification. Indian Journal of Law and Legal Research.
[26] Patil, S. S., & Mishra, S. P. (2026, February 17). Deepfake pornography and criminal law of India: The crises of legal classification. Indian Journal of Law and Legal Research

impersonation, and disinformation, do not specifically address the complexity of artificial intelligence-generated synthetic content. This results in disjointed solutions that don't deal with problems specific to deepfakes, like malicious fabrication, digital permissions, and non-consensual intimate content.[27]

Furthermore, because the Indian criminal laws do not specifically address the harmful production and distribution of these synthetic media forms, there are lesser incentives for prosecution. Platform liabilities and intermediary responsibilities are another significant obstacle. Despite imposing the due diligence criteria and requiring of social media corporations to promptly delete illegal content, the IT Rules, 2021 and their 2025 modifications face enforcement issues and constitutional arguments pertaining to the freedom of expression.

Watermarking and labeling deep fake data are examples of transparency requirements that are very new and lack strong compliance mechanisms. Further the scams and misleading information are more likely to affect people who lack digital knowledge and the public awareness of the deep fakes. India urgently needs a comprehensive deep fake law that balances the innovation, privacy, and the security without restricting free speech, given the stark contrast between the glacial rate of legislative reform and the rapid advancements in technology. In order to give victims tailored legal remedies, strengthen intermediary accountability, enhance forensic capabilities, and create clear statutory definitions, India's current legal system's basic but inadequate handling of deep fake concerns need quick reforms. Without them, deep fake abuse will continue to exploit legal gaps and institutional flaws, jeopardizing privacy, democracy, and public trust.[28]

Chapter- 4- International Comparative Analysis

Moving furhter, the comparative analyses of worldwide legal frameworks for deepfake regulation shed light on how various legal systems address the various issues raised by synthetic media. As deepfake technology spreads rapidly, foreign authorities have implemented a variety of tactics that are influenced by their social norms, technological settings, and legal standards. Notable jurisdictions with a range of regulatory laws include the United States, the European Union, China, the United Kingdom, South Korea, Japan, and Australia. These policies range from decentralized state-level prohibitions to comprehensive, risk-based AI programs and centralized control. This analysis finds differences in enforcement tactics, constitutional interpretations, and user rights as well as convergences including the emphasis on transparency, the need to flag synthetic content, and platform accountability. Understanding of different global models provides crucial insights for developing balanced, context-sensitive laws for countries like India that want to protect their citizens from the harmful impacts of deepfakes while also fostering technology innovation and respecting fundamental rights.[29]

4.1 The United States of America

The USA's approach to deep fake regulation is characterized by an expanding patchwork of state-level laws and potential federal legislation, each addressing a unique detrimental feature of synthetic media. California is the state with the most significant regulations, such AB 730 (2019), which prohibits the unapproved distribution of deep fake films containing sexually explicit content. Another crucial provision is AB 602, which allows victims of deep fake pornography to file civil lawsuits. Other jurisdictions, such as Texas and New York, have passed laws prohibiting the creation and dissemination of deep

[27]Suruchi. (2025, November 9). Deepfakes and the law: A comprehensive comparative analysis of Indian and international legal frameworks. Indian Journal of Law and Legal Research.

[28] Suruchi. (2025, November 9). Deepfakes and the law: A comprehensive comparative analysis of Indian and international legal frameworks. Indian Journal of Law and Legal Research.

[29] Suruchi. (2025, November 9). Deepfakes and the law: A comprehensive comparative analysis of Indian and international legal frameworks. Indian Journal of Law and Legal Research.

fakes without authorization, with a focus on election-related propaganda and private images. The Deep fakes Accountability Act is an important proposed federal law that requires transparent disclosures of content generated or altered by artificial intelligence in order to protect consumers from fraud. The legal tool set consists of the Department of Justice prosecution of fraud legislation relevant to deep fake-related frauds and the Federal Trade Commission enforcement of basic consumer protection laws. The tight balance between the regulation and the First Amendment rights is highlighted by the August 2025 federal court ruling that overturned California's AB 2655, which aimed to mandate platform takedown of the substantially false election materials. This is a significant illustration of how judicial rulings have been impacted by constitutional rights for free expression. Hence , the US regulation, which is backed by extensive enforcement of consumer protection laws, combines the proposed federal transparency measures like the Deep Fakes Accountability Act with the particular criminal penalties and civil remedies like California's AB 730 and AB 602. This varied legislative environment reflects both strong state-level innovation and intricate constitutional considerations regulating deep fake media.[30]

4.2 United Kingdom

The primary law in the UK that addresses offenses or attacks against computer systems, like the hacking or the denial of service, is the Computer Misuse Act 1990. The bulk of crimes against the victims in the present era are related to the disclosure of private sexual photos without consent, cyber stalking and harassment, and offenses involving coercive and controlling behavior. In addition to planning and executing violent acts, people are threatened, controlled, and humiliated through online digital activity. According to the Sexual Offenses Act of 2003, criminals may use social media or online dating services to arrange encounters with the victims in order to commit rape and other sexual offenses. This is comparable to online romance fraud. In 2013, the End Violence Against Women Coalition collected testimonies at a round table on the prosecution and enforcement of online violence and harassment. They expressed serious concerns that the criminal justice authorities handled the online violence and harassment differently and less successfully than they did offline. The National Centre for Cyber stalking Research was established in the UK in 2009 to conduct research and analysis on the prevalence, causes, effects, and the risk assessment of cyber violence against women and girls. To find out how common revenge porn is and what impact it has, the center is currently conducting a poll. In 2011, the institute published the findings of a research on the prevalence, traits, and consequences of cyber stalking.

The primary legislation governing the processing of personal data in the UK is the Data Protection Act of 2018, which is put into effect in conjunction with the United Kingdom General Data Protection Regulation. This framework for the data protection governs every aspect of how companies, organizations, and governmental entities manage personal data. The DPA 2018 mandates that all UK data controllers, or companies and organizations that manage the processing of the personal data, establish and maintain appropriate security measures to protect personal data.

The Online Safety Act of 2023 was passed by the UK parliament to regulate the internet and online safety and to combat cyber crimes. This is one of the English statutes that has measures to penalize deep fakes and down of pornography. The Act aimed to establish the UK as the safest and secure place to be online. Regardless if the perpetrator intended to offend or humiliate the victim, the Bill stipulates that violators will face severe punishment. Part 10 of the Act, which takes effect on January 31, 2024, introduces a number of new communication offenses for anyone who use the messaging services, dating apps, and, social media

[30] Suruchi. (2025, November 9). Deepfakes and the law: A comprehensive comparative analysis of Indian and international legal frameworks. Indian Journal of Law and Legal Research.

platforms, or airdrops to deliver harmful communications. The Act's Part 10 will apply retroactively. Messages transmitted via social media, dating applications, and device-to-device sharing are examples of these infractions. In addition to a possible two-year jail sentence, offenders face a fine. The Act's crimes aim to make the internet a safer environment by addressing the growing incidence of the digital and online abuse. Thus far, prosecutors have tended to oppose these actions by pointing to common law or statute charges, like harassment, that are inappropriate for specific online behaviour.[31]

4.3 The European Union

The European Union has the most thorough and well-organized regulatory approach to handling deep fake technology according to its landmark Artificial Intelligence Act, which aims to create international standards for AI regulation. By classifying AI applications based on their potential to violate basic rights and societal interests, the AI Act establishes a risk-based regulatory framework. It will start to be deployed gradually in 2024. Deep fakes are expressly addressed by provisions demanding responsibility, transparency, and user protection, indicating the European Union's cautious stance to AI concerns. A crucial element is the AI Act's transparency criteria, which require producers and implementing units of AI systems that generate deep fake or artificially altered content to make it clear to consumers that the content was developed or altered artificially. This disclosure should be easy to understand, transparent, and available so that customers may discern between authentic and fraudulent information. The Act requires deep fakes to be technically labeled or watermarked in order to promote accountability and traceability, which discourages misuse and increases digital literacy. Furthermore, the AI Act imposes stringent governance requirements on documentation, compliance evaluations, and human supervision for high-risk AI applications such as deep fake pornography, synthetic media used for political impact, and security-sensitive scenarios. By allowing enforcement agencies to levy harsh fines for infractions, the AI Act pushes platforms and developers to include detection and preventive strategies into their AI ecosystems. The EU aims to boost trust in AI by enforcing the uniform transparency standards amongst their member states, combating misinformation, and protecting individual rights. This Act's ethical and legal improvements place the EU at the forefront of international efforts to control deep fakes by striking a balance between technical innovation and strong protections for democracy, privacy, and free speech in the digital era. The EU AI Act emphasis on mandatory disclosures, watermarking, risk-based governance, and legal responsibility provide a comprehensive framework for tackling deep fake concerns. For other nations considering regulating synthetic media, this framework can be an important reference.[32]

4.4 China

China has established a stringent legal framework for deep fake technology with its Administration of the Deep Synthesis Internet Information Services provisions, which entered into force in January 2023. When it comes to the artificial intelligence-generated synthetic media, these policies prioritize transparency, accountability, and control in order to prevent misuse and foster innovation. An essential component of the system is the mandated labeling and digital watermarking of deep fake video, which requires operators to correctly identify any artificially generated media in order to distinguish it from legitimate content. Further to guarantee traceability and public trust, these labels must be prominently displayed and comprise at least 10% of the visual or auditory material. The restrictions also mandate that the deep synthesis service providers register with Chinese authorities, keep an eye on AI models, and put strict content moderation procedures in place to prevent the spread of illicit or hazardous synthetic content. China's unwavering hostility to malevolent

[31] Ibid.

[32] Suruchi. (2025, November 9). Deepfakes and the law: A comprehensive comparative analysis of Indian and international legal frameworks. Indian Journal of Law and Legal Research.

synthetic media is demonstrated by the requirement that users who create or distribute deep fakes register their true names and the severe penalties, which include fines and criminal prosecutions. In contrast to the European Union's AI Act, which takes a more risk-based and technology-neutral approach along with a few exclusions for artistic usage, China's limits are severe, centralized, and unconditional, with a focus on societal stability and state control. Although both frameworks seek to protect democratic integrity and individual rights, China's approach calls for stricter labeling, user authentication, and a proactive examination throughout the life cycle of AI-driven material.[33]

4.5 South Korea, Australia, and Japan

South Korea, Australia, and Japan all have different legislative approaches to the problems caused by deep fake technology due to their unique socio-legal situations and technological goals. In South Korea, the laws governing deep fakes are primarily concerned with privacy and image protection. The Personal Information Protection Act and the Act on the Special Cases Concerning the Punishment of Sexual Crimes, both of which impose severe penalties on the creation and distribution of non-consensual synthetic explicit media, address deep fake pornography. South Korea stands out for its proactive enforcement policies and digital literacy programs that teach individuals how to spot and report deep fake violations. Further, the constitutional protections that strike a balance between expression and privacy are important when drafting the legislation that seeks to prevent harm while upholding fundamental liberties. Australia has taken a holistic approach, incorporating deep fake issues within existing laws that address image-based abuse, cyber crime, and defamation.Enhancing Online Safety Act, 2015 was modified to add provisions that forbid the improper use of private photos, including artificial intelligence-generated deep fake content. The e-Safety Commissioner is in charge of enforcement, which includes assessing requests for content removal and penalizing businesses that permit harm and ensure digital protection of people.[34]

4.6 What can India adopt from these Global Statutes

India can find a lot of important comparative insights from the global deep fake technology regulatory landscape, which will aid in the development of an efficient legal and legislative response to the unique problems presented by synthetic media. Analyzing the countries like the US, the EU, China, the UK, South Korea, Japan, and Australia reveals those parallels and gaps that India can utilize to build its obscene content regulations and technological protections. The rapidlyly expanding state laws of the United States serve as an example of the efficacy of focused, harm-specific policies that address the non-consensual deep fake pornography. Through adding some specific deep fake regulations to the current cyber laws, India can ensure targeted remedies and strong enforcement. The US experience further highlights the importance of civil remedies for enhancing criminal penalties and encouraging victim empowerment. Further, the AI Act of the European Union offers an advanced, standardized framework that prioritizes risk-based control of AI systems, required watermarking, and transparency. The imposing of compliance duties on AI developers, platforms, and requiring clear disclosures of synthetic content, are some principles that can greatly enhance India's regulatory framework.

The EU's focus on human monitoring and compliance evaluations provides India with a useful foundation for putting accountability measures in place at every stage of the AI life cycle. Moving forward, the efficacy of stringent, centralized control focused on required labelling, the user verification, and content tracking is demonstrated by China's Deep Synthesis Provisions. The emphasis of the Chinese model on the real-name user registration and the technical

[33] Suruchi. (2025, November 9). Deepfakes and the law: A comprehensive comparative analysis of Indian and international legal frameworks. Indian Journal of Law and Legal Research.

[34] Suruchi. (2025, November 9). Deepfakes and the law: A comprehensive comparative analysis of Indian and international legal frameworks. Indian Journal of Law and Legal Research.

watermarking can be adopted to enhance India's current legislative framework, especially in terms of curbing abuses made possible by anonymity, even though the country's democratic context requires better protection of expression and privacy rights.

Next, by combining the criminal sanctions with strict platform accountability enforced by the designated regulator, the UK's Online Safety Act demonstrates proactive control of malicious synthetic content and non consensual deep fakes. This integrated enforcement paradigm, which combines criminal legislation with regulatory monitoring to ensure the timely material removal and the victim restitution, can be the basis for India's future techno-legal crackdown. Lastly, the South Korea, Australia, and Japan's laws offer different viewpoints on how to strike a balance between legislative change and privacy, victim care, and public education and all of these are crucial in India's digital economy. These legal structures of these countries shows the importance of technology cooperation and public awareness to strengthen the legislative actions. India can gain a hybrid legal system that incorporates significant privacy protections and promotes cooperative governance while combining the targeted statutes of the United States, the transparency and the risk-driven mandates of the European Union, the rigorous labelling and tracking practices of China, and the enforcement regime of the United Kingdom. Through creating a robust digital ecosystem that fosters innovation while firmly preventing abuse also, this type of a customized model will more effectively address the various harms that these deep fakes pose for the people . [35]

Chapter- 5: The Path Ahead for India

5.1 Why is the present legal system failing?

Before addressing the specific flaws in India's statutory framework,we need to identify the three fundamental tensions between the nature of the profound fake injury and the organizing presumptions of the present legal system. These tensions are not accidental features of the regulatory landscape. Any legal remedy that disregards them will duplicate the same flaws in a new way since they are systemic. When taken as a whole, they make clear why deepfake pornography is not merely an old harm in a new media but rather a truly unique kind of wrong that requires truly original legal reasoning. The first tension is categorical in character and arises at the level of the legal classification itself. The fundamental principle of the laws currently in place regarding injurious speech and images is that the information that is in question has some connection to an underlying reality, albeit a distorted one. Defamation law raises the issue that whether a statement is untrue. The obscenity legislation deals with the issue of whether content is offensive. Privacy law raises the issue of information disclosure without authority. A factual statement, authentic picture, or real personal information is the first step in any legal investigation. This assumption is totally undermined by deepfakes. They are not inaccurate depictions of reality. They are imitations designed to fit in. When speaking legally, any deepfake content does not represent a false statement about a specific person. It is a false depiction that mimics visual evidence from the real world. This distinction goes beyond simple semantics. It has a direct impact on how each element of an offense or the cause of action is formulated, as well as what kind of proof a victim must offer to establish the wrong. The second problem is jurisdictional, and it arises not between nations but between legal domains. At least four legal frameworks are simultaneously violated by non-consensual deepfake pornography: intellectual property law because the generated image uses aspects of a person's identity as raw material; criminal law because it intentionally causes sexual harm; privacy law because it involves the unconsented appropriation of a person's biometric likeness; and an intermediary liability law because these platforms host and distribute such explicit content. Each of these law systems offers a partial explanation of what went

[35] Suruchi. (2025, November 9). Deepfakes and the law: A comprehensive comparative analysis of Indian and international legal frameworks. Indian Journal of Law and Legal Research.

wrong rather than a complete one. When pursuing remedy through all available channels, a victim must traverse the courts and tribunals with their varied procedural requirements, the standards of proof, and the remedial powers. The complete financial and psychological cost of this fragmented legal system falls on the person who has already suffered harm.

This jurisdictional incoherence is not present in deepfake legislation in particular. It is the result of the legal system that has gathered answers to specific damages without ever creating a cohesive framework for sexual violence enabled by technology. Among the three tensions, temporal tension is the third and possibly the most significant. Because it categorizes and addresses harms which have already been recognized, theorized, and argued, law is intrinsically retroactive.[36] Because technology is naturally forward-thinking, the development of the AI-based synthetic media systems has continuously outpaced the ability of legislators to react. It was unimaginable to the drafters of the Information Technology Act 2000 that a convincingly fake video of any individual could be produced in a matter of minutes using openly accessible software. The 2008 changes were introduced prior to deep fakes being a real-world issue. The 2023 regulatory action recognized the issue but did not take legislative action to solve it. As a result, the legal system is constantly catching up, implementing clauses intended to address various damages in the hopes that they will expand to address the current one. The three tensions—temporal, jurisdictional, and categorical—are not separate.

Without a precise definition of the harm, a legislator will create measures that are incompatible with current legislation and will be out of date by the time they have been passed. Legislative negligence or simple ignorance is not the cause of India's present framework's shortcomings. They are the result of trying to use legal tools that were created for a different context to address a truly original harm.[37]

5.2Structural Drawbacks of the Present Framework

1.Inadequate Definition

Every step of a legal process is rendered unclear by the lack of a definition. When a police officer receives a complaint regarding deep fake content, they must decide whether to file a formal complaint under any applicable provisions. The charge must be framed by a prosecutor. Whether the behaviour is covered by the section must be decided by the court. Definition ambiguity allows harm to slip through the gaps at every stage and, most importantly, gives accused people and their attorneys the chance to claim that the behavior is just not covered by any current legislation. This is not any speculative issue. Police officers refuse to file formal complaints in deepfake cases on the grounds that they are unsure which provision applies, according to advocates working with the survivors of technology-facilitated violence in India. Numerous incidents of these deepfake victims being turned away at police stations or being told to file under sections that have little bearing on the real harm caused have been reported by the Cyber Peace Foundation. A practical gap in enforcement results from the law's definitional vacuum. The 2023 Amendment Rules target the intermediaries rather than the creators and utilize the term deep fake without providing a definition. The core wrong—the act of creation—remains exactly where there is a definitional gap.[38]

2.The Burden of Evidence and Investigation Structure

For most complainants, the evidentiary burden on the victim of deep fake pornography is exorbitant, even in cases where a relevant provision may be found. The official standard of evidence and the actual investigative ability to fulfill it the two levels at which the problem functions. A victim must identify and

[36] International Journal for Legal Research and Analysis. (2026). Volume 3, Issue 1 (March 2026).
[37] International Journal for Legal Research and Analysis. (2026). Volume 3, Issue 1 (March 2026).
[38] International Journal for Legal Research and Analysis. (2026). Volume 3, Issue 1 (March 2026).

connect the accused to the production or dissemination of the content in order to establish the case under any of the aforementioned rules. The perpetrator of a deep fake typically uses VPNs, pseudonymous social media identities, and frequently servers outside of India to operate anonymously. The majority of district-level police units do not yet have the legal authority and the technical capacity necessary for forensic digital investigation, which is necessary for attribution. Although the Cyber Crime Coordination Center is an advance over previous ad hoc setups, it lacks the deep fake-specific forensic toolkit necessary for an efficient investigation. Additionally, India lacks a nationally standardized process for the investigation of the AI-generated sexual damage. This issue is made worse by the IT Act's Section 79 intermediary liability safe harbour.

Once contacted, platforms are encouraged and legally obligated to remove information. They are not necessary to help identify the creator, though. As a result, content may be taken down without any legal repercussions for the offender. Because the media can be re-uploaded and the criminal is likely to target more victims if they are not caught, this asymmetry is especially severe in deep fake scenarios. In practice, the criminal standard of proofthat is the proof beyond a reasonable doubt is strict, and in theory, is correct. The systematic availability of the investigative infrastructure, including the cross-border mutual legal aid,the forensic AI attribution analysis, and real-time platform cooperation that are necessary to meet that criterion in a deepfake case, is lacking in India. Because of this, there is a structural imbalance; although technologically sophisticated wrongdoers can exploit the evidentiary gap, victims bear entire responsibility for the flaws in the legal system.[39]

3.Inadequate Remedies

The remedies offered by the current system are inadequate in three ways: they are incredibly slow to address the damage, they are insufficiently compensatory in comparison to the harm caused, and they are unable to address the ongoing and scattered nature of the suffering. Speed is disproportionately essential in deepfake applications. With each hour that the content is still available, the harm, which includes psychological distress, professional disruption, and reputation damage, increases. The typical timescales in the legal system are counted in months and years, starting with the filing of a formal complaint and ending with an investigation, prosecution, and adjudication. In contrast, a deep fake video can receive tens of thousands of the views in a few of hours after it is posted. The current legal structure in India does not contain any provisions that are comparable to an emergency in civil injunction intended expressly for digital sexual harm. Although civil courts have the inherent authority to award injunctive relief, there are often significant procedural barriers to getting emergency orders against anonymous defendants using international platforms.

The IT Act's Sections 43 and 43A compensation structure was not intended for sexual injury, but rather for data breaches and unauthorized access. The actual and documented harm caused by non-consensual deep fake pornography, such as severe psychological trauma, lost professional opportunities, ongoing monitoring and the removal costs, and the long-term reputation damage that endures even after content is removed, is not reflected in the amount of civil damages available under these provisions. The ongoing nature of the deep fake harm is not addressed by any of the current solutions. Any synthetic video can be saved, uploaded again, and shared endlessly after it has been produced and shared. A criminal conviction corrects the wrong done in the past, but it doesn't stop the harm from continuing. The development of a hash-based database that platforms can utilize to stop re-uploads, the destruction of the primary AI model, or the removal of biometric training data are not required under Indian law. These technological, forward-thinking remedies are completely absent from the Indian legal system and

[39] Ibid.

are being debated more and more in other jurisdictions.[40]

5.3Deepfake Regulation 2025

Changes in the Information Technology (Intermediary Guidelines and the Digital Media Ethics Code) Rules, 2021 were announced on October 22, 2025, by the Ministry of Electronics and Information Technology. India now has its first comprehensive legal framework for handling artificially generated data thanks to these modifications. They signify a change in the way that digital governance operates. The goal of the regulatory framework is to achieve a balance between protecting innovation and controlling deepfakes. It accomplishes this by providing precise definitions, transparency protocols, and platform accountability standards. The changes provide formal statutory recognition for synthetically generated information, which is defined as information that is purposefully or algorithmically created, generated, updated, or modified using a computer resource in a way that appears to be reasonably genuine or truthful. Deep fake audio with altered vocal characteristics, algorithmically modified photos, fake metadata structures, and artificially produced text are all included in this broad description. Regulators are aware of the growing threat posed by deep fakes. Conventional judicial systems are unable to keep up. The ability to create has become more accessible thanks to generative AI techniques. Even performers with no technical knowledge can now use sophisticated deep fake technology. The changes address this fact with language that is neutral toward technology. In order to prevent the regulations from becoming outdated when innovation picks up speed, technology-specific terminology should be avoided.

Core Regulations

1. Statutory Meaning and Extent -The IT Rules framework's acknowledgment of synthetically generated information is codified in New Rule 2(1)(wa). In order to avoid jurisdictional disputes that deep fakes are outside the regulatory purview, New Rule 3(1A) makes it clear that any reference to information in the regulatory terms covering rules regulating the illegal acts, intermediary due diligence, and grievance mechanisms now knowingly includes synthetic content
2. Requirements for Mandatory Labelling -The Amendment requires synthetic content to be fully labelled. Intermediaries offering content generating tools are required by New Rule 3(3) to mark content in a systematic manner. Information created artificially needs to have lasting, distinct metadata. Labels for visual information must always be displayed and take up at least 10% of the screen. Labels must take up the first ten percent of audio content, and neither intermediaries nor end users may change or remove labels. At first glance, this transparency sets genuine stuff apart from fake. Over the course of a deep fake video, significant AI-generated labels span one-tenth of the frame area.[41] Audio deepfakes need to be audibly disclosed in the first few seconds so that viewers may evaluate the content's authenticity. The regulatory conclusion that an informed consumer is a crucial harm-mitigation strategy is reflected in this system.
3. The Intermediary Liabilities and Requirement for SSMI - The tool suppliers must mark synthetic outputs, add distinctive identifiers that enable traceability, and ensure that the labels are visible and permanent before distributing them to users. By addressing the proliferation at the source rather than through the downstream distribution, this upstream responsibility transfers accountability from passive platforms to active technology suppliers. The Significant Social Media Intermediaries (SSMIs) that have five million or more active users each month are required to get user statements on the creation of synthetic material. Platforms must deploy reasonable

[40] International Journal for Legal Research and Analysis. (2026). Volume 3, Issue 1 (March 2026).
[41] Arya, K. (2025, December 16). Deepfake regulation India 2025: MeitY's comprehensive IT rules amendment. Khurana & Khurana, Advocates and IP Attorneys.

technical measures verifying declarations through automated content analysis or human review protocols. SSMIs that remove synthetic content in good faith based on the reasonable attempts or user complaints are protected by the statutory safe harbour in new Rule 3(1A). This protection promotes quick response mechanisms that strike a balance between user rights and platform capabilities, while acknowledging that platforms cannot accomplish immediate removal in the pandemic-scale content areas.[42]

5.4 Suggestions and Recommendations

This paper's analysis shows a clear trend toward legislative reform across jurisdictions: victim-centered, targeted laws that criminalize the production and dissemination of the non-consensual deep fake pornography, along with expedited administrative removal procedures and easily accessible civil remedies. Recognizing that legislative reform alone is insufficient, the following suggestions are put forth. Accessible legal aid, judicial training, and enforcement capability are all equally important.

However, the most basic issue that can be resolved right away is the lack of appropriate legislation. First, India needs a particular law that makes the production and dissemination of the non-consensual synthetic intimate imagery illegalIdeally, this law should be an update to the IT Act or a chapter inside the BNS. While keeping a degree of the technological neutrality to accommodate future developments, the clause must be sufficiently explicit to provide investigators and prosecutors with unambiguous guidance.

The definition of covered content should place more emphasis on the harm that is, the representation of an identifiable original person in the sexual content without that person's consent than on the specific technological methods of creation. Second,the mens rea importance should be predicated on non-consent rather than intent to harm. An accused person who creates a deepfake of a real person without that person's consent should not be able to avoid responsibility by arguing that their objective was self-gratification rather than purposeful pain of the victim. To prove the mental component of the crime, it should be enough to know that the content features an original person and that consent has not been acquired. This standard eliminates the enforcement shortcomings noted in early US state legislation and is in line with the strategy of the United Kingdom's Criminal Justice Act 2025.[43] Third: The Korean Communications Standards Commission's methodology should serve as the blueprint for the fast-track administrative content removal system. Intermediaries should be legally obligated to remove reported deep fake content within 24 to 48 hours of receiving notice under this method, which should function without depending on the criminal justice system. In order to stop previously deleted content from being uploaded again, the mechanism should additionally mandate that platforms use hash-based detection techniques. Fourth, victims should have a separate civil right of action with a rebuttable presumption of harm upon demonstration of the creation and of distribution. This relieves victims of the burden of individually demonstrating the extent of the psychological and reputation harm in civil proceedings—a challenging and traumatizing process. The civil remedy needs to be offered in addition to criminal prosecution, not in instead of it. Fifth, the DPDP Act needs to be changed to specifically acknowledge the use of an individual's biometric information, including photos, to train artificial intelligence models that produce personalized synthetic graphics. The Data Protection Board should have the authority to issue emergency orders to this effect, and victims should have a compulsory right to seek the removal of both created content and the underlying training data.[44]

[42] Arya, K. (2025, December 16). Deepfake regulation India 2025: MeitY's comprehensive IT rules amendment. Khurana & Khurana, Advocates and IP Attorneys.

[43] International Journal for Legal Research and Analysis. (2026). Volume 3, Issue 1 (March 2026).

[44] Ibid.

5.5 Other Suggestions

Firstly, in terms of setting clear constraints on those acts, national standards and a well-amended or designed Personal Data Protection Act can make these activities more manageable. Then, the regulatory agencies should use Deep fake detectors to keep an eye on the veracity of online data. Thirdly, the best defense against the malevolent usage of Deep fake generators is a well-defined legislation. Fourth, preventive actions should be implemented in addition to penalties for past offenses. Lastly, in these situations, an investigation should be conducted to identify the perpetrator and hold them accountable.[45]

Conclusion

Non-consensual deep fake pornography causes real, serious harm that disproportionately affects the victims. It is expanding as well. Over the past three years, the technology that makes it possible has become significantly more accessible. Anyone with a smartphone, a stable internet connection, and a downloaded application may now perform tasks that formerly needed significant computational power and technological know-how. The technological capabilities that are available to those who would hurt victims and the legal framework available to victims are becoming more and more dissimilar. Victims are failed at every stage of the legal process by India's current framework, which is a patchwork of statutes written for various harms and implemented with the interpretive uncertainty by investigative processes insufficient to the task. They are let down at the definition level since the particular injury caused by artificial intimate pictures is not explicitly covered by any current legislation. Because the infrastructure needed to identify and prosecute deep fake offenses is not consistently available, it fails them at the evidentiary level. Additionally, it fails them at the remedial phase too since no current solution is quick enough, thorough enough, or progressive enough to deal with the persistent and widespread nature of deep fake injury. These flaws have been recognized by lawmakers in countries including the US, South Korea, and the UK, who have taken decisive action to address them with a particular legislation. India hasn't.

The 2023 Ministerial Advice and the Amendment Rules acknowledge the issue but these are not the remedy. Finding a solution requires legislation that clearly defines wrong, recognizes harm, holds manufacturers and distributors accountable, provides victims with prompt and convenient remedies, and provides enforcement agencies with the tools they need to carry out effective investigations. The question is not whether such legislation will be necessary in India. Technology exists, there is a recognized legal void, and widespread harm is occurring. The question is, how many victims will be disappointed by the present law system before such legislation is passed?[46]

*****

[45] Magizhini. (2025). Deepfake regulation, legal framework & its ethical dilemmas. IJLES.

[46] International Journal for Legal Research and Analysis. (2026). Volume 3, Issue 1 (March 2026).