Vol. 1, Issue 1, August 2024 Subject-Law ISSN 3049-3099 (Print)

VIPS JOURNAL OF LAW & DEVELOPMENT

VIVEKANANDA INSTITUTE OF PROFESSIONAL STUDIES-TC (VIPS-TC)
Affiliated to GGSIP University, Delhi & Approved by Bar Council of India & AICTE
Grade 'A++' Accredited Institution by NAAC &
Recognized by UGC under Section 2 (f) & NBA Accredited for MCA Programme
ISO 9001:2015 Certified Institution

About Vivekananda Institute of Professional Studies – TC (VIPS-TC)

Vivekananda Institute of Professional Studies - TC (VIPS-TC) was established in the year 2000. Even as a sapling, its roots were firm, for they were energized by Swamiji's teachings. Today, VIPS – TC has progressed and is nestling sixteen courses under seven different Schools. It continues to stand with determination, moral sight and strength of mind to create capable and ethical human beings with infinite power, infinite knowledge and indomitable positive energy. Under the aegis of VIPS – TC, Vivekananda School of Law and Legal Studies (VSLLS) is committed to realizing the words of Swami Vivekananda: "Man Making, Character Building and Nation Building" and is well known for its robust efforts in legal education. Research is integral to academics as it forms the foundation for knowledge creation and intellectual growth. It enables students, scholars, and professionals to explore new concepts, test theories, and contribute to the existing body of knowledge in their respective fields. VSLLS works towards development oriented research in the Legal domain.

About the VIPS Journal of Law & Development

VIPS Journal of Law & Development is an annual double blinded peer reviewed journal accepting submissions in English language. The inception year of the Journal is 2024 and it is further envisioned to promote global development of Law as it provides a platform for scholarly research dedicated to exploring the intersection of legal frameworks and socio-legal development with an inter disciplinary approach. The research articles are selected for publication after a rigorous double blind review by subject experts. The mode of citation for the journal is VIPS VSLLS VOL I VJLD (2024). As a policy of the Journal the contributing authors are regularly updated about the status of their submission.

Table of Contents

Title of the Paper / Author	Page No.
From State Control to Market Forces: Reformation of Indian Coal Sector *Dr. Manoj Kumar Singh & Dr. Priya Bhatnagar*	1
Global Economic Interdependence: Evaluating the UNCITRAL Model Law and Adaptive Frameworks for Cross Border Bankruptcy *Dr. Parineeta Goswami & Arushi Goswami*	11
Tokenization of Digital Collectibles: Analysing Regulatory Framework and Legal Challenges Related to Non-Fungible Tokens *Purva Kaushik*	33
Plastic Politics and Need for Maintaining Sustainability: Initiatives by Nilkamal Limited a Leading Company in India's Plastic Industry *Adv. Rajat Jain & Dr. Nipun Gupta Jain*	48
The Sabarimala Matter: A Way Forward *Adv. R. Karthik & Dr. J Ravindran*	61
Gender neutrality in boardrooms of Indian Companies: An Analysis *Adv. Abhishek Grover & Dr. Honey Sharma*	76
Sexual Offences Against Transgenders: An Unresolved Puzzle *Priyansha Badoni & Sonali Sharma*	90
Innovation Barriers and Poverty: Analysing the Socioeconomic Implications of Patent Systems *Aaditya Bajpai & Shreya Bajpai*	101
Beyond Morphing - Unravelling Deepfake Technology and Its Legal Analysis *Priyal Bansal & Chandra Kant Singh*	114
Cryptocurrency Regulation in India *Arman Sheikh*	132

BEYOND MORPHING- UNRAVELLING DEEPFAKE TECHNOLOGY AND ITS LEGAL ANALYSIS

Priyal Bansal*
Chandra Kant Singh**

VIPS Journal of Law & Development
Subject - Law
August 2024, Vol. 1, Issue 1, 114-131
ISSN 3049-3099 (Print)
©Vivekananda Institute of Professional Studies-TC
(VIPS-TC)
https://vips.edu/vslls/Publications/VJLD

ABSTRACT

'When reality meets fabrication and ethical reality shifts, it is then deepfake creeps in.' Artificial Intelligence has evolved extensively from life-soothing to life-distorting techniques by producing an illusion that, while initially seeming real, is a trick of the light. The pseudo-reality is nothing more than a deepfake that has created havoc lately on social media, which is not just limited to victimising Indian actors and politicians but celebrities across the globe. Deepfake, the most summarised form, is a technologically advanced form of digital deceit utilising ritualistic intelligence to convincingly alter visual-aid auditory contests, often leading to realistic impersonations and challenging traditional means of verifications. The authors scrutinise the existing legal landscape in India concerning deepfake technology. Interpreting current laws related to privacy, cybercrime, intellectual property, and information technology identifies the gaps and inadequacies hindering the effective regulation of deepfake. The research paper deliberates on the balance between freedom of expression and the need to prevent malicious use of growing technology, offering insights into how the legal framework can strive for equilibrium.

Keywords- *Artificial Intelligence, Data Protection, Privacy, Cybercrime, Legislation.*

* Student of BA LLB at RMLNLU, Lucknow
** Student of BA LLB at RMLNLU, Lucknow

I. INTRODUCTION

The entire geopolitics world was taken aback when a video purportedly displayed Ukrainian President Volodymr Zelenskyy[1] urged his compatriots to surrender to the Russian army. However, to everyone's surprise, it was a fabricated video generated using machine learning technology, and his voice and video clips were used to create an illusion. The technology in the picture is Deepfake, which involves machine learning, i.e., Generative Adversarial Networks (GAN). It will be a bolt from the blue if someone says today that they have never encountered a deepfake. Yes, maybe the technical terminology associated would have kept them unaware. Still, in the everyday world, in some form or another, we come across bogus and fabricated videos, images, and audio, which often go unnoticed as spurious. Such is the efficiency of tech geeks, slang for technological experts.

Oxford described deepfake[2] as: '*Any of various media, esp. a video, that has been digitally manipulated to replace one person's likeness convincingly with that of another, often used maliciously to show someone doing something that he or she did not do.*' This term originated when a Reddit moderator created a subreddit named 'deepfakes' where they posted face-swapped videos of celebrities as pornographic videos.[2] Synthetic media comes with a bittersweet combination as it has some significant advantages that go unnoticed by the masses. The technology can be used in education, where historical figures' speeches or videos could be recreated for better understanding or used in entertainment by aiding in VFX and CGI processes to create more realistic scenes.[3] It is impossible to overlook the negative aspects, from scamming and dissemination of false news to promoting fake pornographic content etc.[4] The bitterness of the technology is more prevalent, and it needs to be clamped down. The latter option could be used as a weapon of deterrence for the deepfake creators, but the same could not be promised until a thorough analysis is concluded. In India,

1 *A Zelensky Deepfake Was Quickly Defeated. The Next One Might Not Be*, WIRED (Mar. 17, 2022, 1:30 PM), https://www.wired.com/story/zelensky-deepfake-facebook-twitter-playbook/. [2] OXFORD ENGLISH DICTIONARY, https://www.oed.com/dictionary/deepfake_n?tl=true.

2 BRITANNICA, https://www.britannica.com/technology/deepfake.

3 Ashish Jaiman, *Positive Use Cases of Synthetic Media (aka Deepfakes)*, MEDIUM (Aug. 15, 2020), https://towardsdatascience.com/positive-use-cases-of-deepfakes-49f510056387.

4 Mehmet Emin Masca, *Advantages and Disadvantages of Deepfake Technology*, MEDIUM (Dec. 3, 2021), https://medium.com/geekculture/advantages-and-disadvantages-of-deepfake-technology-ccfa7c12b1ae. [9] Matt Novak, *Viral Video Of Actress Rashmika Mandanna Actually AI Deepfake*, FORBES (Nov. 5, 2023, 03:09 PM), https://www.forbes.com/sites/mattnovak/2023/11/05/viral-video-of-actress-rashmika-mandanna-actuallyai-deepfake/?sh=6267d8847232.

Deepfakes fall under the jurisdiction of the Information Act, 2000; Indian Penal Code, 1860; Digital Personal Data Protection Act, 2023; and Information Technology Rules, 2021, as there is no specific legislation dealing with Deepfakes. States of USA-Washington, Texas, and New York laws are examined thoroughly, and favourable characteristics are highlighted that might inspire Indian lawmakers to enact better rules in the nation. Plausible solutions to the issues found in the existing laws are given to bridge the gap.

II. A National Perspective on the Legal Challenges in Implementation

Deepfake is a term that has been in the limelight lately owing to the incident with Rashmika Mandanna[9], a renowned Bollywood actress, where a video of her being involved in sexual activities went viral. The video was said to be fake, and it was generated using deep learning algorithms and Generative Adversarial Networks (GAN).[5] Possibly, this is not the first instance of the misuse of this technology, and the victims have ranged from the entertainment industry to the politics of nations by circulating morphed videos of politicians. Instances of misuse of deepfakes have substantiated the fact that the technology could be misused. If the same is not regulated soon, perhaps a catastrophe is imminent. The Union Minister for Electronics and Information Technology (MeitY), Ashwini Vaishnav, has, to some extent, addressed the issue. It is evident that the government has taken cognisance of the issue and is possibly working on it.[6] However, the amount of time required to formalise these concepts is enormous, and due to the rapid rise[7] in deepfake cases, laws regulating the practice must be developed. There could be grave repercussions if the government does not propose new legislation or amend current legislation that could, to some extent, prosecute and create a state of deterrence amongst the perpetrators.

Although there isn't a specific law in India that addresses deepfake in the present scenario, there have been some prior laws that may partially address the issue. A few

5 Shubham Pandey and Gaurav Jadhav, *Emerging Technologies and Law: Legal Status of Tackling Crimes Relating to Deepfakes in India*, SCC ONLINE BLOG (Mar. 17, 2023), https://www.scconline.com/blog/post/2023/03/17/emerging-technologies-and-law-legal-status-of-tacklingcrimes-relating-to-deepfakes-in-india/.

6 *Ibid.*

7 *Sumsub Research: Global Deepfake Incidents Surge Tenfold from 2022 to 2023*, SUMSUB (Nov. 28,2023), https://sumsub.com/newsroom/sumsub-research-global-deepfake-incidents-surge-tenfold-from-2022-to-2023/.

rules that indirectly deal with deepfake are the Information Technology Act,2000; the Indian Penal Code, 1860; and the Digital Personal Data Protection Act, 2023.

A plausible dilemma might arise in the minds of lawmakers and citizens regarding-

i. Are the present laws capable of dealing with deepfakes?

ii. If not, is there a need for separate legislation or amendment in the present laws will suffice?

To answer these questions, the research paper presents a thorough analysis of the existing laws.

2.1 Information Technology Act, 2000: A Thorough Analysis

The adage "old is gold" is accurate in many facets of life. Still, due to evolving circumstances and recent technological developments, the authors cannot make the same assurances about the laws. Only a few must-have predicted in 2000 that, twenty years later, technology would emerge, changing our perception of reality. This frightening development needs immediate remedy, and one law that might address the problem of deepfake is the Information Technology Act of 2000. However, it will be difficult to conclude anything without a study of the act.

a. Nexus between Section 66D[8] and Section 66C[9]

Section 66D states, '*Punishment for cheating by personation by using computer resource Whoever, by means of any communication device or computer resource, cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees,*' The perplexity is to establish a link between personation and deepfake. To begin with, the definition of personation is – *'to act or play the part of'*[10] Understanding the definition of deepfake in detail will help one establish the association. Deepfake[11] is defined as using technology to create the appearance that a natural person has done or said something when, in fact, it was not done at all, and this is what personation means. To make this appear natural, the identity of the targeted person

8 The Information Technology Act, 2000, §66D.

9 The Information Technology Act, 2000, §66C.

10 COLLINS, https://www.collinsdictionary.com/dictionary/english/personate.

11 MERRIAM- WEBSTER, https://www.merriam-webster.com/dictionary/deepfake.

is stolen. This implies that that person's identity was stolen. The same is covered under Section 66C, which reads as *'Punishment for identity theft. "Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh."*

The video in which the American President, Joe Biden,[12] was seen making transphobic remarks, which could be one example of identity stealing. At first, it may seem that the provision is a way to penalise illegal deepfake creators, but it has a significant flaw. The flaw is that there is no mention of the machine learning algorithms that deepfake uses to generate its results, which could provide an opportunity for the offenders to escape.

b. Section 66E[13]

Referring to the previously given example of Rashmika Mandanna[21], another sub-section of this provision came into the picture when the Delhi Police filed the case in a matter under Section 66E.

Section 66E reads as: *'Punishment for violation of privacy.–Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.'* Applying the provision in the instance of deepfake is complicated.

The actual distinction is made by the sentence, "publishes or transmits the image of a private area of any person without his or her consent." It states that publishing or transmitting an image of that person's private parts is illegal. Still, in deepfake pornography cases, the person targeted is not the one whose private parts are exposed—instead, it is someone else's. This defeats the argument that the targeted person's right to privacy is being violated by disclosing their private parts; instead, the private parts of the person whose face is superimposed in the video are exposed.

12 *False claims of 'deepfake' President Biden go viral*, BBC (July 28, 2022), https://www.bbc.com/news/62338593.

13 The Information Technology Act, 2000, §66E. [21] *Id* at 3.

c. Section 67[14]

Women have been the primary target of deepfakes in the form of revenge, as 96 per cent of deepfake cases fall under the category mentioned above.[15] Following the publication of lewd films and images of female influencers, such as Alia Bhatt[24] and Katrina Kaif[16], one may wonder if any existing Indian laws could protect them from publishing such lascivious content.

Section 67 may provide some insight regarding the same.

However, since it doesn't explicitly mention deepfakes, people might be unable to associate with it. The creators of revenge porn will be covered in this provision as in the line '*if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it*'. When someone uses deepfake to create revenge porn, their face is superimposed on the body of the person engaging in sexual activity. This gives the illusion that the targeted person is engaging in the activity, which damages the reputation due to the difficulty of concluding if the information is real or fake. Sections 67A[17] and 67B[18] will apply to the victim who is a major and a minor, respectively.

d. Section 72[19]

The definition of privacy has always been subjective and contentious. According to Cambridge University[29], privacy is "the state of being alone." This suggests that the essence of privacy is the ability to be left alone. However, deepfakes have seriously shaken this concept by controlling

14 The Information Technology Act, 2000, §67.

15 Sally Adee, *World's First Deepfake Audit Counts Videos and Tools on the Open Web*, IEEE SPECTRUM (Oct. 7, 2019), https://spectrum.ieee.org/the-worlds-first-audit-of-deepfake-videos-and-tools-on-the-open-web. [24] Bijin Jose, *Alia Bhatt is the latest to fall prey to deepfakes: 12 ways to stay safe online*, THE INDIAN EXPRESS (Nov. 30, 2023, 8:32 AM), https://indianexpress.com/article/technology/artificial-intelligence/alia-bhattdeepfake-video-ways-to-stay-safe-online-9045902/.

16 *Katrina Kaif is latest victim of deepfake tech after Rashmika Mandanna, fake pic of diva from 'Tiger 3' goes viral*, THE ECONOMIC TIMES (Nov. 10, 2023, 04:07 PM), https://economictimes.indiatimes.com/magazines/panache/now-katrina-kaif-is-latest-victim-of-deepfake-techtowel-clad-pic-from-tiger-3-goes-viral/articleshow/105040415.cms?from=mdr.

17 The Information Technology Act, 2000, §67A.

18 The Information Technology Act, 2000, §67B.

19 The Information Technology Act, 2000, §72. [29] CAMBRIDGE DICTIONARY, https://dictionary.cambridge.org/dictionary/english/privacy#google_vignette.

people's privacy by sharing any image, video, or audio without permission, infringing on their fundamental right to privacy.

As stated in the above statement, Section 72 may address this issue.: "*Penalty for Breach of confidentiality and privacy***.–**'*Save as otherwise provided in this Act or any other law for the time being in force, if any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.*'

The gaps in this provision are listed as follows:

i. Absence of contemporary sources: The primary sources used by the makers of deepfakes are images, videos, and audio files. These are not mentioned at all. While it is possible to cover these sources if we read between the lines of the clause, it is best to state clearly which sources might get misused.

ii. Inadequate Punishment: Another problem with this clause is that the maximum sentence of two years is inadequate. Because of the invasion of privacy and the unfathomable effects it could have on the victim, this is a significant offence with dire consequences.

2.2 Digital Personal Data Protection Act, 2023

Social media platforms have been the chief source for disseminating deepfakes since they have become a convenient way for offenders to reach a large audience, notably when the topic is contentious or involves a well-known personality. This implies an urgent need to regulate social media platforms to curb the spreading of the matter as soon as possible. Digital Personal Data

Protection Act (DPDP), 2023 is one recent law that may partially cover the issue of Deepfake as it is concerned with the protection of an individual's data from misuse by Data Fiduciaries or social media platforms.[20]

20 Sarvagya Chitranshi, *The "Deepfake" Conundrum - Can the Digital Personal Data Protection Act, 2023 Deal with Misuse of Generative AI?,* INDIAN JOURNAL OF LAW AND TECHNOLOGY (Dec. 23, 2023), https://www.ijlt.in/post/the-deepfake-conundrum-can-the-digital-personal-data-

a. Applicability of the DPDP Act

Sections 3(a)[21] and 3(b)[22] The Act will apply if the processing is carried out in India and outside the country. Still, ambiguity could be traced in section 3(c), which deals with the non-applicability of this act.

Section 3(c)(i)[23]- This clause states that: *'not apply to— (i) personal data processed by an individual for any personal or domestic purpose'*. This poses the question of what is meant by

'personal or domestic purpose'. A crucial question about deepfake could be raised, i.e., how will the common populace be protected in case of a personal data breach if there is ambiguity in the definitions of *personal or domestic purpose* under this act? Initially, the act promised the protection of individuals' data and its lawful usage by processing it.

Section 3(c)(ii)[24]- This brings another question of doubt regarding the applicability of the act.

It states: '*not apply to —*

(ii) personal data that is made or caused to be made publicly available by—

(A) the Data Principal to whom such personal data relates.'

Therefore, the data publicly made available by the *Data Principal* would not be covered under the ambit of this clause. Here, Data Principal[39] 'means the individual to whom the personal data relates'. One of the most significant problems concerning the act is that Data principals will not be protected if they publicly make the data available, which defeats the legislation's purpose. Most affected by this clause would be prominent personalities from various fields, such as entertainment, politics, sports, etc., who publicly upload their data.

protection-act-2023-deal-withmisuse-of-ge.

21 The Digital Personal Data Protection Act, 2023, §3(a).

22 The Digital Personal Data Protection Act, 2023, §3(b).

23 The Digital Personal Data Protection Act, 2023, §3(c)(i).

24 The Digital Personal Data Protection Act, 2023, §3(c)(ii). [39] The Digital Personal Data Protection Act, 2023, §2(j).

2.3 Indian Penal Code, 1860

The Indian Penal Code serves as the foundational legal framework governing criminal offences in India. Its various provisions indirectly involve the concerns raised by the sophisticated form of deception. In this context, IPC's provisions related to defamation, obscenity, cheating by personation, and forgery become crucial in navigating the legal structure surrounding deepfake. The discussion will delve into specific sections of IPC, shedding light on the legal intricacies and ensuring the legal system works in tandem with the evolving technology.

a. Section 124A[25] and Section 499[26]

Section 124A criminalises acts that express hatred or contempt towards the government established by law, whereas Section 499 deals with defamation, aiming to protect individuals' reputations from harm. Section 124A says, "*Whoever by words, either spoken or written, or by signs, or by visible representation, or otherwise, brings or attempts to bring into hatred or contempt, or excites or attempts to excite disaffection towards, the Government established by law in India, shall be punished with imprisonment for life, to which fine may be added, or with imprisonment which may extend to three years, to which fine may be added, or with fine.*"

Section 499 reads, "*Whoever, by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the cases hereinafter excepted, to defame that person*."

However, there are challenges to attract sedition and defamation as a penalised provision for deepfakes:

i. Ambiguity in definition- The inherent ambiguity in the definition of sedition has already raised concerns, and incorporating yet another aspect dealing with deepfake into it without explicitly mentioning it may lead to controversies and differing interpretations. Section 499 prevents individual-centric defamation; deepfake offences may target groups and organisations or contribute to broader societal discord. Thus, the provision may fall short.

25 The Indian Penal Code, 1860, §124A.

26 The Indian Penal Code, 1860, §499.

ii. Communication modalities- The sections primarily focus on written or spoken communication, making it less suitable for addressing offences involving manipulated content characteristics of deepfakes. In other words, the provisions' language will not suffice the diverse forms of communication associated with synthetic media.

iii. Proving malicious intent- The criminal law is often expressed by the Latin phrase, "*actus non facit reum nisi mens sit rea*", loosely translating into an act that does not make a man guilty of a crime unless his mind is also guilty. It is challenging to prove the creator's intent as sometimes the deepfake could be created in satire or fun without the intent to harm someone's reputation. For instance, the increasing trend on social media to add songs in the form of memes (an amusing or interesting item such as a captioned picture or video or genre of items that is spread widely online primarily through social media)[27] as if sung by the Prime Minister, Mr Narendra Modi.

A similar reasoning is to attract Sections 501[28] and 502[29], which regard printing and sale of defamatory matters as unlawful, which is difficult to establish as the provisions contain the words "*known to be defamatory*." The term 'matter' in the sections traditionally does not involve manipulated or created content; this can again lead to debate due to the conventional understanding of matter and not having an absolute mention of deepfake. In short, the courts may face difficulties applying these sections to offences involving deepfake content, as the sections have not considered the ambit of digital manipulation.

b. Section 292[45]

The section constitutes the legal framework that addresses offences related to obscenity in India. The section reads as follows, "*A book, pamphlet, paper, writing, drawing, painting representation, figure or any other object shall be deemed to be obscene if it is lascivious or appeals to the prurient interest or if its effect or where it comprises two or more distinct items, the effect of any of its items, is, if taken as a whole, such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.*"

27 MERRIAM- WEBSTER, https://www.merriam-webster.com/dictionary/meme.

28 The Indian Penal Code, 1860, §501.

29 The Indian Penal Code, 1860, §502. [45] The Indian Penal Code, 1860, §292.

The provision encompasses a broad spectrum of materials, encompassing various forms of expressions, and the essence of obscenity, according to the section, lies in lascivious content, appeals to prurient interests, or has an overall effect that tends to deprave and corrupt individuals who are likely to encounter it. The words are subjective in themselves and do not explicitly define what constitutes obscenity and do not outline the criteria for determining whether particular materials are deemed obscene.

Notably, the provision indirectly includes the concept of fake and created content when it says, "*comprises of two or more distinct items*"; however, despite the seemingly comprehensive nature of the section, its applicability is confined to physical and tangible items. The limitation arises from the wording of the section, which refers to "*any other object.*" This phrasing, while broad, does not explicitly extend to encompass digital or virtual content, which has become increasingly prevalent in the modern era.

As a result, the effectiveness of Section 292 in addressing offences related to fake and created content, especially in digital form, is constrained. The legal consequences for such content being treated as obscene under the IPC are not fully realised due to the legislative gap concerning the inclusion of digital content within the ambit.

c. Section 509[49]

The provision reads, "*Whoever, intending to insult the modesty of any woman, utters any words, makes any sound or gesture, or exhibits any object, intending that such word or sound shall be heard, or that such gesture or object shall be seen, by such woman, or intrudes upon the privacy of such woman, shall be punished with simple imprisonment for a term which may extend to three years, and also with fine.*"

There is a recognised gap in these laws when it comes to addressing sexual harassment through electronic means, such as deepfake crimes. Deepfake involves using technology to create realistic-looking but fabricated content, often for malicious purposes, and can include creating explicit and non-consensual material. In the context of the existing law, the absence of specific provisions addressing electronic modes of harassment, like deepfake crimes, is a significant limitation. The law was formulated in an era when electronic communication methods were less prevalent today. As a result,

the law does not adequately cover the nuances and challenges of modern technology, making it essential to revisit and update legal frameworks to address emerging forms of harassment.

The initiative was taken by Chhattisgarh to insert clause 509B[30], which specifically addresses sexual harassment by electronic means, is commendable. The state amendment recognises the evolving nature of crimes in the digital era and aims to provide legal protection to individuals who may be targeted through online platforms. For adequate and uniform protection against online sexual harassment, it is crucial for other states and, ideally, the national legislature to consider similar amendments to their legal frameworks. This would ensure that individuals nationwide have consistent legal recourse against offences committed through electronic modes.

III. The Legal Landscape of the United States for Deepfakes

India isn't the only nation grappling to regulate deepfakes; instead, multiple nations have stepped up to mitigate the problem promptly because of the damage deepfakes are doing to countries. The United States of America (USA) was one of the first nations where regulation of deepfakes began by enactment of the National Defense Authorization Act for Fiscal Year 2020.[31] Further, states like New York, California, Washington, Texas, Georgia, etc., also participated in regulating deepfakes by enacting their laws. These laws must be scrutinised to check whether they are geared up or if some issues need to be fixed. Furthermore, inspiration could be drawn from these laws by Indian lawmakers to close the gaps mentioned in the research paper.

3.1 Washington Deepfake Law

The Senate of Washington passed a law on April 6th, 2023, relating to defining synthetic media in campaigns for elective office and providing relief for candidates and campaigns. The primary object of the act is to shield a candidate from any synthetic media usage that might be against the said candidate and provide reasonable damage caused by the act. The abstract spirit behind the law is to strengthen democratic elections by curbing any illegal usage of artificial intelligence

30 The Indian Penal Code, 1860, §509B.

31 Jason C. Chipman and Stephon W. Preston, *First Federal Legislation on Deepfakes Signed Into Law*, WILMERHALE (Dec. 23, 2019), https://www.wilmerhale.com/insights/client-alerts/20191223-first-federallegislation-on-deepfakes-signed-into-law.

(AI) that might hamper the smooth voting process.

a. Accuracy of the Definition

Synthetic Media[32]: The definition of synthetic media has been beautifully drafted as it covers all the aspects that might be misused, such as image, video, or audio through AI. Further, it mentions the mechanism used to create deepfakes, i.e., the Generative Adversarial Network (GAN). It reads as: *'an image, an audio recording, or a video recording of an individual's appearance, et speech, or conduct that has been intentionally manipulated with the use of generative adversarial network techniques or other digital technology'*. Later, Section 2(1)(a)[33]and Section 2(1)(b)[34] state how deepfakes might be used, i.e. to deceive or create a fundamentally different impression of action, appearance, etc. Section 2(1)(a) and Section 2(1)(b) read as:

> *(a) A depiction that to a reasonable individual is of a real individual in appearance, action, or speech that did not actually occur in reality; and*
>
> *(b) A fundamentally different understanding or impression of the appearance, action, or speech than a reasonable person would have from the unaltered, original version of the image, audio recording, or video recording.*

At this junction, the above-mentioned definition of synthetic or fabricated media is perfect as it covers all the domains of deepfakes. Inspiration could be taken from this definition by Indian lawmakers while amending previous legislation or drafting a new law regarding deepfakes. Inserting a definition like those mentioned above would enable the encapsulation of the data or media produced by deepfakes, which could be penalised if they are illegal.

Relief to the victim: Remedy of injunction is provided under Section 2(2), which reads as: '*seek injunctive or other equitable relief prohibiting the publication of such synthetic media'*. The remedy for damages is covered under Section 2(3).

The remedies provided under the abovementioned provisions are civil, which prima facie appears to be adequate. However, this might not be appropriate because of

32 42, R.C.W. § 2(1) (2023).

33 42, R.C.W. § 2(1)(a) (2023).

34 42, R.C.W. § 2(1)(a) (2023).

the danger and damage this technology's usage might cause to the whole nation or world. 2024 is a crucial year in the political world due to the significant elections across nations from India, the USA, Indonesia, Russia, and many more.[35]

After the entry of deepfakes into the political realm, it is very important to put penal measures to create deterrence in the minds of illegal deepfake creators. The addition of criminal punishment could be one way to solve this problem.

3.2 Texas[36]

Chapter 21 of the Penal Code of Texas has been amended by adding Section 21.165 to read as follows- '*Unlawful Production Or Distribution Of Certain Sexually Explicit Videos.*' The act came into effect on September 1, 2023. The act defines deepfake video as '*a video, created with the intent to deceive, that appears to depict a real person performing an action that did not occur in reality.*' The elements of the crime include-

- The person produces or distributes a deepfake.
- It depicts the person with exposed intimate parts or engaged in sexual conduct.
- The action is done without the effective consent of the person.

While this amendment is a step towards addressing the issues related to deepfake videos, it is crucial to take note of its limitation, which is its limited scope-The amendment explicitly targets deepfake videos and does not extend its ambit to cover other forms of deepfake like photographs and audio recordings. The current law will not address the misleading and falsified photographs and synthetic voices, potentially misleading to false representation and deception.

3.3 New York

Kathy Hochul, the Governor of New York, signed Senate Bill 1042A[37] on September 29, 2023.[38] The Act is about the unlawful dissemination or publication of intimate images created by digitisation and of sexually explicit depictions of an individual.

35 Koh Ewe, *The Ultimate Election Year: All the Elections Around the World in 2024*, TIME (Dec. 28, 2023, 10:30 PM), https://time.com/6550920/world-elections-2024/.

36 Texas Penal Code, § 21, cl. 165 (2023).

37 New York Penal Law, §245.15.

38 Zach Williams, *New York bans deepfake revenge porn distribution as AI use grows,* BLOOMBERG LAW (Oct. 2, 2023, 10:07 PM) https://news.bloomberglaw.com/in-house-counsel/n-y-outlaws-unlawful-publication-ofdeepfake-revenge-porn.

The legislation intends to protect individuals from maliciously distributing private and explicit content without their consent.

Section 1 of 245.15 of the penal law includes the elements:

- The person must intend to cause harm to another individual. The individual must disseminate the still or video image.
- The person must be reasonably identifiable from the image or information displayed in connection.

The issue left uncovered is limiting content to images and video images, leaving out other forms of explicit content, such as audio recordings, synthetic writings, or any representations.

Section 2 explains digitisation as '*to alter an image in a realistic manner utilizing an image or images of a person, other than the person depicted, or computer generated images.*' The definition is wide in its ambit as it encapsulates all computer-generated images; an amendment to not restrict it to images but videos and other forms of media will bridge the potential gaps in protection. The language expansion would enhance the law's relevance and effectiveness in addressing a more comprehensive range of digital manipulations.

Although the provisions are not flawless, inspiration should be drawn from them to introduce laws against deepfakes in India.

IV. Solutions

Deepfake technology has ushered in a new era of digital deception, posing significant privacy and information security threats. As technology becomes more sophisticated, addressing this challenge requires a multifaceted approach, which includes legal, technological and societal dimensions.

4.1 Awareness Amongst Masses[39]

Public awareness is a critical component in the fight against the manipulation of media content. The rising threat of deepfake technology necessitates efforts to raise public awareness and equip individuals with the knowledge needed to navigate the digital landscape. The following ways could help generate awareness.

39 Mika Wesrerlund, *The Emergence of Deepfake Technology: A Review*, 9 T. I. M. REV. 39, 45 (2019).

a. Educating the general population about the existence, capabilities, and potential dangers of deepfake technology is essential. Many individuals become susceptible to misinformation and manipulation due to a lack of awareness.

   Educational institutions should cover the basics of creating deepfakes, their potential applications, and their risks.

b. Governments, Non-Governmental Organisations, and technological companies should collaborate to implement widespread awareness campaigns. Each sector brings unique strengths, and collaboration would ensure comprehensive dissemination of information; as in this case, the Government can provide framework and support, NGOs can leverage networks, and companies can provide their platforms to reach vast audiences.

c. The central aspect of spreading awareness is empowering individuals to evaluate the authenticity of media content critically and fostering a mindset that does not accept everything at face value, creating a collective defence against deepfakes.

4.2 Amendments in present laws to give inclusivity to deepfakes[40]

Incorporating specific language that explicitly identifies deepfake-related offences and recognising the distinctive nature of these crimes would ensure a robust legal response to deepfakes.

a. To enhance legal clarity and precision, amendments should incorporate terms like 'deepfake' into the definitions section of relevant laws. This will ensure that the language of the legislation reflects the technology it seeks to regulate and will establish a clear framework for judicial interpretation.

b. The lawmakers should work closely in collaboration with technology experts to understand the technical intricacies of deepfake creation and detection.

c. Preventive measures like stringent licensing requirements for deepfake creation tools should be incorporated to minimise the occurrence and

40 Jack Langa, Deepfakes, Real Consequences: Crafting Legislation to Combat Threats Posed by Deepfake, 101 B.U.L. REV. 761, 797 (2021).

opportunity for everyone to indulge in malicious activities.

d. Engaging with international counterparts, sharing best practices and knowledge to collectively prosecute against cross-border deepfake offences due to the global nature of the internet and digital content sharing.

4.3 Stricter Punishments-

To effectively counter the malicious use of deepfakes, it is imperative to establish a legal framework that not only identifies and defines offences related to deepfakes but also imposes stricter punishments on those engaged in the activities. It will punish the wrongdoers for their actions and deter potential offenders from participating in the illegal act.

- The offenders should face substantial fines and imprisonment as punishment. The severity of these legal consequences should be proportionate to the potential harm caused by deepfake.
- Legal frameworks should be subjected to periodic review as the technology evolves, and so should the legal responses. Lawmakers should proactively identify the challenges and assess the effectiveness of existing laws to make necessary adjustments.

4.4 Investments in Research and Development[41]

A strategic initiative for staying ahead of the curve is crucial, ensuring the country is well-equipped to detect deepfakes effectively. It calls for governments, private companies, and academic institutions to make substantive investments in research and development.

a. Machine learning stands at the forefront against deepfakes. Investments should be directed towards advancing machine learning algorithms.

b. Research in forensic analysis tools should also be prioritised to establish reliable methods for tracing the source of false content.

c. Public-private partnerships will create a synergy, accelerating the development of detection.

41 Danielle K. Citron & Robert Chesney, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 CAL. L. REV. 1753 (2019).

d. An integrated approach ensuring a comprehensive coverage of different mediums like audio, video or photograph should be adopted.

In conclusion, by implementing the comprehensive strategy, society and law can build a resilient defence against the growing threat of deepfakes. Acknowledging the vulnerabilities of individuals, investing in research and development, enhancing legal framework, fostering collaborative efforts, and creating awareness can create safeguards in the digital age. Through these proactive measures, one can mitigate the risks posed by deepfakes and ensure a secure digital environment.

V. Conclusion

The detrimental power to damage one's reputation or shake the whole democracy of a nation is imminent if left untouched. Deepfake technology has ushered in a new era of challenges and opportunities. In the time when Urfi Javed and Ranveer Singh were not only brutally trolled but were also facing criminal charges, even when they posted their real pictures online. When the issue changes to creating pictures, videos, or audio, why will the situation not turn chaotic? The deceptive nature of the technology cannot be ignored as it poses privacy threats, and vigilance is crucial to detect and counteract the damaging effect of deepfakes. Drawing insights from the American jurisdiction, the paper provides a roadmap for Indian lawmakers to consider when crafting comprehensive legislation. As we navigate this complex terrain, a proactive approach is imperative to safeguard the integrity of information and uphold the trust of interconnected world allies.



VIPS
योगः कर्मसु कौशलम्
IN PURSUIT OF PERFECTION

NAAC Accredited A++ Grade 3.58/4

VIVEKANANDA INSTITUTE OF PROFESSIONAL STUDIES-TC (VIPS-TC)

AU Block (Outer Ring Road), Pitampura, Delhi-110034
Nearest Metro Station – Pitampura (2 KM) & Haiderpur (0.5 KM)
Website : www.vips.edu, www.dsb.edu.in
Tel.: +91 11 27343401 / 02 / 03, Fax : +91 11 27343404
E-mail : vslls.clrd@vips.edu