DEEPFAKES AND MISAPPROPRIATION OF IDENTITY: LEGAL REMEDIES AND CHALLENGES

Shubham Verma, Ph.D. Scholar, University of Lucknow, Lucknow

Surbhi Khurana, Ph.D. Scholar, Gujarat National Law University, Gandhinagar

Shobhit Sainesh Awasthi, Ph.D. Scholar, Dr. RML National Law University, Lucknow

ABSTRACT

The proliferation of deepfake technology - audio, video or images created by advanced artificial intelligence (AI) systems - has significantly transformed the contemporary media landscape. This technology offers new opportunities for the entertainment, educational, outreach and creative industries in generating realistic deepfake media. Deepfakes may also be used as a tool to propagate disinformation, defame reputation, facilitate identity theft, and also tamper with voting systems and cyber security systems. The increasing sophistication and difficulty of spotting such content further exacerbates the risks to human dignity, democracy and trust.

In India, the current legislative framework, such as the provisions under information technology, criminal and civil laws, in part, address the harms but does not explicitly regulate and control the generation, distribution and abuse of deepfake content. The lack of a dedicated legislative framework results in enforcement, victim and platform accountability shortcomings. This paper maps the technological basis of deepfakes, such as machine learning and neural networks, to gain insight into the extent and nature of the problem. It examines the socio-legal aspects of synthetic media, especially with regard to privacy, freedom of speech and reputation. By comparison with regulatory developments in selected foreign jurisdictions, the study identifies best practices and potential policy pathways. Ultimately, it argues for a rights-oriented and technologically informed legal framework that is able to balance innovation with constitutional safeguards in the emerging digital environment.

Keywords: Deepfake Technology, Misinformation, Digital Rights, Cyber Law, Regulatory Reform.

1. Introduction

The modern digital age is changing the sphere of public discourse more and more due to online sources, instant communication, and the excessive distribution of visual materials. The unprecedented rise of social media has presented new avenues of expression and innovation; however, it has also caused the boundary between reality and fabrication more than any other time to be weak. One of the most disturbing trends in this environment is the emergence of so-called deepfakes, the extremely advanced digital fakes produced using the latest artificial intelligence technologies, such as the so-called generative adversarial networks (GANs) and other models based on machine learning. The technologies make it possible to produce videos, audio recordings and images that are convincing replicas of the face, voice and mannerism of a person to a point that they may puzzle even trained observers[1].

Synthetic media seems to be an incredible technological breakthrough at the face of it. It has potentials in applications in cinema, education, language translation, accessibility by persons with disabilities, and digital preservation. But, the same tools can be utilized in a creative and constructive way, and may be used against people as well. The use of deepfakes has become widespread to spread fake news, destroy reputations, commit financial fraud, and generate explicit non-consent media. They have been leveraged to masquerade as representatives of the government, influence political discourses and corrupt elections. By doing this, they not only jeopardize the dignity and privacy of individuals, they also undermine the legitimacy of democratic institutions as well as the quality of debate in the public. In contrast to the traditional methods of misinformation, which in many cases may be proved by means of fact-checking or contextual explanation, deepfakes are based on visual and auditory misleading. They take advantage of the natural human behaviour to believe what we see and hear. Because of this, they subvert popular confidence in the real media, which creates a larger phenomenon of the liar dividend, in which even true facts can be refused as fake. The implication of this loss of trust spreads far and wide in governance, law enforcement, journalism, and administration of justice[2].

The Indian response to deepfakes is highly indirect and disjointed in terms of legal consideration. Currently, no specific law exists that governs the development or distribution or

[1] Einola S, Kohtamäki M and Hietikko H, "Open Strategy in a Smart City" (2019) 9 Technology Innovation Management Review 35 <https://doi.org/10.22215/timreview/1267>

[2] De Ruiter A, "The Distinct Wrong of Deepfakes" (2021) 34 Philosophy & Technology 1311 <https://doi.org/10.1007/s13347-021-00459-2>

abuse of AI-generated synthetic media. Disgruntled parties have to depend on a patchwork of available stipulations in Information Technology Act, 2000, Indian Penal Code, 1860 now Bharatiya Nyaya Sanhita 2023 (BNS) and other supporting laws. Although BNS provisions concerning recognition of digital records, severe penalties for organized cybercrime (Section 111), enhanced protections against digital voyeurism (Section 77), online stalking (Section 78), and Defamation and Digital Publications (Section 356) could be used in the proper cases, but other special laws were created when the manipulation of content with artificial intelligence was unpredictable. They are therefore in many instances ineffective in responding to the extent, velocity, and intricacy of damage inflicted by deepfakes. Now, what should the law do regarding the freedom of speech and expression and the necessity to curb the digital harm? How far must intermediaries be blamed to be a host or amplifier of synthetic content? All these issues require a thoughtful government policy and a proactive legal solution, which acknowledges both the potential of AI to bring about change and the potential of AI to be abused[3].

This paper will have a detailed analysis of the legal solutions that are presently available in India to solve the problem of deepfakes and similar types of misinformation. It evaluates the sufficiency and weakness in the current statutory provisions, judges the judicial reactions where relevant, and pinpoints the significant voids in imposition and compensation to the victims. Moreover, it also compares the experience of other jurisdictions that have initiated the implementation of specific laws or regulation platforms on synthetic media and AI responsibility. The paper aims to evaluate the ways in which India can develop a principled and effective regulation strategy by examining world trends and good practices. The research paper suggests a systematic legislative plan of regulating AI-controlled synthetic media in India. It proposes a fair structure that would protect the basic rights and maintain accountability, transparency and technological responsibility. By doing that, the paper will be contributing to the wider discussion about digital governance and the dire necessity to defend the democratic ideals in a more synthetic information space[4].

2. Understanding Deepfakes and Misinformation

Deepfakes are a developing type of synthetic media that has been developed by utilizing

[3] Fallis D, "The Epistemic Threat of Deepfakes" (2020) 34 Philosophy & Technology 623 <https://doi.org/10.1007/s13347-020-00419-2>

[4] Nema P, "Understanding Copyright Issues Entailing Deepfakes in India" [2021] International Journal of Law and Information Technology <https://doi.org/10.1093/ijlit/eaab007>

powerful artificial intelligence. Through studying facial expressions, speech patterns, and minor body movements, these systems are able to produce highly realistic results that are in close resemblance to the face and mannerisms of an actual person. The outcome is media content which can be convincingly realistic to the common consumer and is frequently hard to tell the difference between actual media and recorded content, unless the content is scrutinised by specialised forensic analysis or technical understanding[5].

There are different types of deepfakes and each one of them poses its own difficulties. One of the most discussed is video deepfakes, which may represent a person who apparently said or did something he or she has never did. They have been employed to spread false political speeches, made misleading public announcements, as well as create non-consensual explicit content. The audio deepfakes do the same, only that they do not modify the visuals, other than that they are used to imitate the voice of a person with impressive precision. Through this technology, fraudsters have been able to pose as business leaders, political figures or relatives to tamper with financial processes or steal confidential data. Image-based deepfakes are the production or manipulation of photographs, and may be used to create social media identities; harm reputations or used as so-called revenge imagery. Moreover, synthetic content created with the help of sophisticated language models can be in the form of a text, which creates a believable and authoritative fabricated news report, a forged statement of the person or a coordinated disinformation campaign.

Misinformation entails the transmission of false or misleading information regardless of whether there is the intention to do the same. In the present global digital age, where information tends to move incredibly fast through social media networks and messaging systems, any manipulated content is in a position to reach large masses of people in a very short span of time. Deepfakes worsen this issue since they cull out the credibility of visual and auditory evidence, which is an evidence form per se that was previously trusted, into question. Consequently, people might find it harder to distinguish between original and fake content which results in confusion, mistrust, and polarisation[6].

The abuse of the deepfake technology has a much wider implication than personal damages. The political arena can be disrupted by fake videos or audio tapes as they flood the electoral

[5] Nema P, "Understanding Copyright Issues Entailing Deepfakes in India" [2021] International Journal of Law and Information Technology <https://doi.org/10.1093/ijlit/eaab007>

[6] Zhao H and others, "Multi-Attentional Deepfake Detection" [2021] IEEE 2185 <https://doi.org/10.1109/cvpr46437.2021.00222>

proceedings with false information about the candidates or government officials. At the individual level, deepfakes have been employed to harass and cyber bully, defame and extort individuals, especially kids, women and prominent figures. Manipulated statements or forged announcements, on economic side, may also result in distorted market behaviour in the stock prices and confidence of investors. With the ever-increasing technological possibilities, the societies are now being forced to address not only the technical aspects of detecting and regulating, but also the ethical implications and legal issues of identity, consent, and accountability in the digital era[7].

3. Legal Framework in India

There is no dedicated special law in the Indian legal system that directly addresses the challenges posed by deepfakes and AI-generated content. Instead, measures should be derived from a combination of existing cyber, criminal and data protection laws. Although these provisions provide partial relief, they were drafted in a technological context that did not anticipate synthetic media or algorithmically manipulated identities[8].

The main legislation regulating online behavior and cyber crimes in India is the Information Technology Act of 2000. Some sections of this Act can be used in connection with deepfake videos. Section 66E penalizes the misuse of privacy in respect to images of a person's private areas being recorded, published, and transmitted without consent. In instances where deepfakes consist of non-consensual intimate images, this section can be applicable. Sections 67 and 67A deal with the publication or transmission of obscene and sexually explicit material in electronic form, which can be used in instances of non-consensual sexually explicit deepfakes transmitted online. Additionally, Section 69A gives the Central Government the authority to deny public access to online content in the interests of sovereignty, integrity, or public order. Although this section can be used to remove problematic deepfake content online, it is basically a content-blocking tool and not a remedy for victims. Importantly, none of these provisions were drafted with artificial intelligence or synthetic media in mind. They do not explicitly address issues such as algorithmic creation, manipulation of consent, liability of creators or intermediaries, or attribution of responsibility in cases where content is generated anonymously or through

[7] Čučilović I, "Deepfake Technology: Criminal Law Implications" (2024) 15 Crimen 325 <https://doi.org/10.5937/crimen2403325c>

[8] Tandy B, "Deepfakes: Identity Misappropriation in the Digital Age" [2025] SSRN Electronic Journal <https://doi.org/10.2139/ssrn.5101133>

automated systems[9].

Extremely important is the introduction of the Digital Personal Data Protection Act, 2023, which is a major change in the privacy regime in India. The Act lays stress on the legitimate treatment of personal information, informed consent, as well as the responsibilities of information custodians. The Act may provide some protection in the case of deepfakes that are made on the basis of illegally acquired personal information - photographs, biometric identifiers, voice samples. Nevertheless, it focuses more on data processing and not content manipulation. It does not directly control the production of artificial or fake content that is simulating an individual without necessarily using illegally acquired information. As a result, while the law theoretically strengthens privacy rights, it leaves unanswered questions related to non-consensual digital impersonation, identity misuse, and the spread of AI-generated false representations[10].

In summary, these legal tools offer a piecemeal and tangential approach to the issue of deepfakes. They offer some avenues for prosecution or removal, but they do not constitute a comprehensive framework that is specifically tailored to address the technical and evidentiary issues of identity manipulation through the use of artificial intelligence. This is a reflection of the increasing need for a statutory framework that is directly linked to synthetic media, and that is specifically concerned with the protection of identity in the digital age.

4. Judicial Interpretation and Legal Remedies

(a) Right to Privacy – *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017)[11]

In *Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)* the code of privacy was established as an inherent constituent of the right to life and personal liberty as guaranteed by Article 21 of the Constitution. This was a path breaking case in the Indian constitutional law that saw the establishment of privacy not just as a negative right against the encroachment of the State but as a positive right that protects personal autonomy, dignity, control over all forms of information and body integrity.

The consequences of such a decision are significant when considering the deepfake technology.

[9] Darma M and others, "Legal Implications of Deepfake Technology Misuse in Digital Content on Social Media" (2025) 2025 Science of Law. 98 <https://doi.org/10.55284/eqazc148>
[10] Kishwar SD and others, "Regulating Deep Fakes and Synthetic Media: Privacy, Policy and Global Regulatory Challenges" (2025) 8 Journal of Data Protection & Privacy. 78 <https://doi.org/10.69554/hbgg8150>
[11] (2017) 10 SCC 1

Deepfakes, particularly the ones including fake intimate content or sexually explicit content generated against the will of the person, are a serious encroachment of the personal space of an individual. It is not just a manipulation of the likeness of the person but the destruction of his dignity, independence and power over his own self. Informational privacy is recognized in the *Puttaswamy*, and it becomes the right of an individual to control the use of his/her personal data and image. The usage of artificial intelligence devices to create fake videos or images with the face or voice of a person without their consent means that this autonomy is literally being denied. Nevertheless, even though this right has good constitutional background as discussed by *Puttaswamy,* the issue of how it can be effectively implemented in deepfake situations is still questionable. As discussed above India does not have a specific statutory framework that is specifically concerned about creating and spreading synthetic media. Victims can only turn to a mixture of constitutional solutions and fragmented statutory laws which in most cases are not sufficient to overcome the speed, anonymity and cross-nationality of digital injuries. Therefore, even though the constitutional right to privacy provides the conceptual protection, the lack of specific laws undermines the effectiveness of its functioning in the digital era[12].

(b) Vishaka Principles and Sexual Harassment Jurisprudence

The evolution of sexual harassment jurisprudence in India, beginning with *Vishaka v. State of Rajasthan* (1997), laid the groundwork for recognising harassment as a violation of fundamental rights under Articles 14, 15, 19, and 21. The Court in *Vishaka* framed guidelines to protect women from sexual harassment at the workplace, emphasising dignity, equality, and a safe environment as constitutional guarantees. These principles were later codified in the Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013. In the current digital landscape, deepfake pornography has emerged as a disturbing extension of gender-based harassment. Women are more likely to be targeted by fake intimate videos or altered pictures that are meant to embarrass, scare, or silence them. People often use this kind of abuse to cyber bully, force someone to do something, or get back at someone[13].

Despite the illegality of obscenity, identity theft, and the dissemination of sexually explicit material in the Bharatiya Nyaya Sanhita and the Information Technology Act of 2000, enforcement of these laws is difficult. Proving identity and intent is a major difficulty.

[12] Asadi O, "Exploring Current and Potential Solutions: The Rise of Deepfakes in Legislative, Legal, and Technological Arenas" (2025) 39 Berkeley Undergraduate Journal <https://doi.org/10.5070/b3.50655>
[13] Sharma K, Li Y and Comite U, "The Rise of Deepfake Fraud," *IEEE* (2025) <https://doi.org/10.4018/979-8-3373-5992-2.ch005>

Anonymous accounts, encryption software, and foreign servers are commonly used by offenders, making it difficult to investigate and prosecute them. Finally, victims may have to shoulder a crushing burden of proof, especially if the digital content spreads rapidly across multiple platforms, making it difficult for law enforcement to intervene. This content often results in psychological, reputational and social damage long after its removal. Although the current jurisprudence on sexual harassment supports the constitutional idea of dignity and equality, it is still developing in relation to technologically advanced forms of harassment such as deepfakes. Questions arise as to how the law can adapt to the phenomenon that harassment is no longer confined to physical or workplace settings; now, it has entered the virtual world where it can be instantaneous and far-reaching.

(c) Absence of a Recognised Right to Be Forgotten

The other major loophole of law in India is, there is no formally recognised Right to Be Forgotten (RTBF). This feature is particularly important when it comes to victims of the online abuse who want harmful information to be removed forever. Even in India, despite the occasional acceptance of the concept by courts in limited contexts, statutory protection of the right to demand complete deletion of digital content does not exist at all. Deepfake victims are thus confronted with a significant challenge of ensuring that they eliminate manufactured content of images or videos permanently once posted into the digital realm. When content is removed on one site, it can be posted on others, and the problem of erasing it becomes ineffective[14].

The lack of a distinct RTBF framework has left the victims reliant on platform-based mechanisms of grievance or judicial orders by bits. This is a reactive strategy that is usually very slow and unpredictable and has minimal promise of a sustained solution. In light of the permanence of digital records and the ease with which content can be copied, bureaucratic legal framework that empowers persons to reclaim their digital identity has become more and more urgent. Though the constitutional jurisprudence on the privacy and dignity issues offers an effective normative framework, the legal solutions to the victims of deepfake abuse are both ad hoc. Core rights such as those involved in such technology have been identified by the judicial interpretation, and the development of the efficient statutory and procedural protections continues.

[14] Lin LSF, "Examining the Role of Deepfake Technology in Organized Fraud: Legal, Security, and Governance Challenges" (2025) 4 Frontiers in Law 6 <https://doi.org/10.6000/2817-2302.2025.04.02>

5. Comparative Legal Approaches

(a) United States

In the United States, regulation of deepfakes has largely developed at the state level, as there is currently no comprehensive federal statute that specifically regulates the creation or dissemination of deepfake content. The lack of a cohesive national framework has resulted in a disjointed legal environment where various states have implemented targeted policies to address particular harms related to manipulated media. Legislation has been passed in states like California, Texas, and Virginia to address two main issues: the proliferation of non-consensual sexual content and the misuse of deepfakes in election processes. Laws pertaining to elections typically forbid the dissemination of deceptive audiovisual content meant to mislead voters within a predetermined window of time prior to an election. By prohibiting the use of phony speeches or campaign messages to sway public opinion, these clauses aim to protect the integrity of elections.

Given the harm that pornographic deepfakes cause victims in terms of psychological distress, reputational damage and privacy concerns, many state laws prohibit the creation and distribution of non-consensual pornographic deepfakes. Such laws often offer protection against technologically sophisticated exploitation by being included in broader statutes on image-based abuse or "revenge porn". Federal legislative efforts are still in the form of proposals. There is growing interest in Congress, as reflected in the proposed Deepfake Accountability Act and the Protect Elections Act. These bills consider measures such as disclosure or watermarking to enhance the ability to detect manipulated content, and criminal penalties for malicious use of deepfakes. These initiatives reflect an awareness of the need for a unified approach to combat the online and transnational spread of deepfakes, despite not being legislated. Rather than developing a comprehensive regulatory framework for artificial intelligence-generated content, the US approach remains piecemeal and focused on certain areas, primarily electoral interference and sexual exploitation.

(b) European Union

The European Union has dealt with the issue of deepfakes as part of a larger effort to protect data, regulate digital governance, and control artificial intelligence. The EU doesn't try to make laws that only deal with deepfakes. Instead, it uses the tools that are already in place, like the General Data Protection Regulation (GDPR), to protect people in a roundabout way.

Individuals have strong rights by the GDPR regarding the processing of their personal data, among other things, the right to erasure (also known as the right to be forgotten), the right to data portability, and processing of their personal data based on a valid law. These protections may be used when a deepfake content is a case where the likeness, voice, or biometric identifiers of another person have been used without his or her permission, which is viewed as an infringement, and to seek compensation against the perpetrator of an unlawful processing.

Besides the data protection law, the EU has shifted to a more formal regulatory framework on artificial intelligence. The suggested Artificial Intelligence Act (AI Act) uses a risk-based framework of AI technologies. In this context some applications of synthetic media can be identified as high-risk applications, especially those that can cause threats to the processes of democracy, of fundamental rights, or security of people. The proposed bill focuses on the transparency requirements, noting that the AI generated or manipulated content should be explicitly reported as such. This practice is an expression of the extending view of the EU which is the protection of human dignity, privacy, and informational autonomy. By regulating deepfakes within the framework of responsible AI governance, the European Union aims to strike a balance between technological innovation and responsibility and the defense of fundamental rights.

(c) China

In order to control deepfake technology, China has taken a more centralized and regulator-driven approach. In 2022, China released specific administrative guidelines on the use of "deep synthesis" technologies. These rules require that to prevent fraud, content created using artificial intelligence (AI) or other synthetic technologies must be identified. Those hosting the content need to establish verification measures, record keeping and ensure the source of the manipulated media can be traced. The regulation imposes various responsibilities on online service providers. Failure to monitor, detect and remove harmful synthetic content could result in liability. Tracing and real-name authentication are consistent with China's broader approach of digital governance that favours platform compliance and state surveillance. By forcing disclosure and imposing compliance costs on the intermediaries, China hopes to eradicate misuse, while allowing for continued government control over the internet. The Chinese system is more focused on monitoring and enforcement, as opposed to the other jurisdictions where it is largely complaint- or civil action-driven.

6. Ethical and Human Rights Considerations

The rapid evolution of deepfakes has resulted in complex ethical and human rights implications. While it is true that artificial intelligence has helped create new ways to innovate and express creativity, the abuse of artificial intelligence to create manipulated, but convincingly realistic, audio, video and images, is a serious threat to human dignity, autonomy and rights. Underlying this issue is consent and autonomy. Deepfakes are a form of identity theft, an unpermitted use of the person's face, voice or image. Using a person's image without their permission to create a fake image is a form of image theft. This is especially concerning when it comes to intimate or sexually explicit images, which can have a disastrous effect on an individual's bodily autonomy and mental health[15].

Freedom of expression is a cornerstone of constitutional democracy and is enshrined in Article 19(1)(a) of the Indian Constitution. Deepfakes can be used to influence elections and deceive the public through the spread of manipulated media presented as valid evidence. The rampant spread of misinformation on social media erodes public trust in governmental institutions, media and even video evidence. Hence, the challenge is in finding the right balance between the regulatory framework developed to manage the use of malicious deepfakes, and freedom of expression. The issue of gender-based violence and exploitation adds yet another layer of human rights considerations associated with deepfakes. Indeed, a significant share of malevolent deepfake content is aimed at women, particularly non-consensual intimate imagery. It helps perpetuate patriarchal tendencies and hinders women in cyberspace. The damage done is not confined to defamation; It may also lead to social isolation, professional failure, and intense emotional harm. In this context, deepfakes have become a technological extension of gender-based violence, demanding a sensitive and victim-centered legal response.

Also important is the right to reputation that is part of the right to life and personal liberty as provided in Article 21 of the Constitution of India. The Supreme Court has on several occasions reasserted that reputation is an aspect of dignity and it cannot be tampered with in a careless manner. Deepfakes are able to create false statements or actions that were not originally made thus ruining the reputation of an individual in the society. When this content spreads online, it becomes very hard to remove and the stigma could linger on even after the truth is realized. Reputational harm resulting through synthetic media should therefore be considered by the law

[15] Kigwiru VK, "Deepfake Technology and Elections in Kenya: Can Legislation Combat the Harm Posed by Deepfakes?" [2022] SSRN Electronic Journal <https://doi.org/10.2139/ssrn.4229272>

as a grave violation of the constitutional rights[16].

It should not be aimed to choke technological innovation or creative expression, but rather have accountability in cases where harm is done. The rules must also include clear definitions, reasonable limits, and enough help for the victims, as well as protections against abuse of censorship powers. It is also important to have preventive measures in place, such as programs to teach people how to use technology safely, making platforms responsible, and using technology to find fake content. The law must also seek to support human dignity, personal freedom, and democratic integrity, and, in addition, innovation. This is important in ensuring that the new technologies are not used against society by violating the basic rights.

7. Differential Societal Impact of Deepfakes and the Emerging Legal Challenges of Identity Misappropriation

Discussing deepfakes and identity misuse: legal remedies and challenges, it is imperative to comprehend that the deepfake technology is not effective in all social spheres. The performances are very different when it comes to entertainment, journalism, education and political communication. Of most concern, however, are the legal implications where the issues of identity, authenticity and trust in the people come into conflict. Deepfake technology has been justified in the entertainment sector as a means of creativity. It helps film-makers, game studios, and digital storytellers to build imaginary worlds at unparalleled speed and minimal cost of production. With the use of artificial intelligence, it is possible to create characters, imitate the voices, and produce the immersions without having to rely solely on the conventional knowledge of graphic design. Companies such as Nvidia have invested in AI-driven production spaces that incorporate the use of generator tools into the gaming and cinematic production process. These inventions represent a new direction in the artistic fields and not their obliteration; the Human skills are not fully outwitted but are re-focused on management, criticism and moral regulation. But in legal terms, there is also the concern of creative usage in terms of consent, intellectual property, the right of the artist and post-mortem identity usage. When the image or voice of an individual is reproduced without his or her consent, what is considered as innovation and what would be considered as identity misuse takes legal importance[17].

[16] Van Der Sloot B and Wagensveld Y, "Deepfakes: Regulatory Challenges for the Synthetic Society" (2022) 46 Computer Law & Security Review 105716 <https://doi.org/10.1016/j.clsr.2022.105716>

[17] Blauth TF, Gstrein OJ and Zwitter A, "Artificial Intelligence Crime: An Overview of Malicious Use and Abuse of AI" (2022) 10 IEEE Access 77110 <https://doi.org/10.1109/access.2022.3191790>

In the case of journalism and news reporting the scenario is much more complicated. The aspect of trust is an essential part of the discourse of democracy, and deepfakes directly attack that aspect. As compared to fiction in entertainment, the news content purports to be authentic and factual. Appearing in a malicious way, synthetic media is capable of creating speeches, interviews or visual evidence which can result in the distortion of the common perception. It is not merely misinformation which is the legal issue in this case, but intentional identity abuse - whereby, public figures, journalists or private people are digitally reproduced saying or doing things they never said, or never did. The result of such manipulation is defamation, intrusion into privacy, loss of reputation, and even tampering with elections. The vulnerability to such deceits is increased in socio-politically less stable societies or those with low media literacy levels, and an imbalanced distribution of harm ensues. The Deepfake technology is a two-sided tool as well. Although this can destroy the credibility of the press, it can also be added to the verification structures by the use of forensic detection tools created by media institutions and public broadcasters. However, this is not a defence in which the legal risks are eliminated. Synthetic materials tend to spread faster than the current regulatory measures can react. According to the existing Indian legal frameworks, either in the information technology legal frameworks, the penal law, or in the developing principles of data protection, the liability is usually reactive, but not proactive. The fact that there is no clear statutory definition of what constitutes a synthetic media or deepfakes makes enforcement and the standards of evidence more difficult.

This is also true of the institutions of learning that are threatened by both opportunity and threat. On the one hand, the simulations created by AIs can be used to enhance pedagogy, particularly in the arts and digital media. Conversely, fake scholastic contents, distorted lectures and counterfeit research documents pose a challenge to academic honesty and sincerity of scientific conversation. When students or teachers fall prey to an identity-fraudulent digital impersonation, the question enters the field of academic ethics into the possibility of legal recovery related to identity theft and reputational harm[18].

Deepfakes have psychological and financial impacts, which further testify to their severity. The sophisticated voice-cloning technologies enable falsified interviews or anonymous quotes to be given a false persona of well-known people. These fake identities have the potential to

[18] Danry V and others, "AI-Generated Characters: Putting Deepfakes to Good Use" [2022] CHI Conference on Human Factors in Computing Systems Extended Abstracts 1 <https://doi.org/10.1145/3491101.3503736>

propagate incitement, manipulate markets or cause communal turmoil. The contagion of such information makes such content even more damaging, particularly in regard to the audience not aware of verification measures. The struggle to prevent the propagation of deepfakes is turning to the same technical design that also allows them to be generated machine learning and neural networks. Detection systems are aimed at detecting abnormalities in facial mapping, pixel distortion, or vocal modulation. It is however, an emerging competition. As generative adversarial networks get more advanced, the detection tools tend to lag. Hence, the law system has a moving target. In comparison to the time - honoured method of image manipulation, a technical skill and a great amount of resources are required, the modern production of deepfakes has become not only economically feasible but also technically easy, and the number of ways to abuse it has grown[19].

Re-contextualized or slightly edited original material is inexpensive counterfeit, and it involves minimal technical manipulation. Deepfakes, in turn, are created using sophisticated AI algorithms using large datasets to recreate the facial expression, voice style, and behavioural subtleties of a person with astounding realism. The distinction does not only lie in the fact that on the one hand, cheap fake products can pass as false claims, on the other hand, deepfakes are the intentional digital impersonation, which creates even stronger allegations of identity abuse and criminal responsibility. The spread of deepfakes in the wider constitutional context engages the basic rights - the right to privacy, the right to dignity, the right to reputation and the right to free speech. The problem is how to give innovation and artistic freedom and retain the people against exploitation of their digital identity. The legal response is still fragmented because there isn't a clear set of laws that defines synthetic media, makes platforms responsible, and gives victims quick ways to get help. So, when you talk about Deepfakes and Identity Abuse: Legal Remedies and Challenges, you're not just talking about how cool technology is; you are also talking about constitutional protections and changes to the law. Deepfakes are more than just a communication problem; they are a structural legal threat to identity, authenticity, and trust in democracy in the digital age.

8. Conclusion

With the rapid development of the field of artificial intelligence, new challenges for the digital environment have emerged in ways that we have never seen before. One of such challenges,

[19] Shahid F and others, ""It Matches My Worldview": Examining Perceptions and Attitudes around Fake Videos" [2022] CHI Conference on Human Factors in Computing Systems 1 <https://doi.org/10.1145/3491102.3517646>

especially nowadays, is the issue of deepfakes. With synthetic media being utilized for deception, in contrast to conventional methods of spreading false information, it's impossible to differentiate between what is true and what is not because it perfectly copies the voices, expressions, and even gestures of its subjects. However, this technology is not just affecting the credibility of the people whose name it's tarnishing. The effects of this kind of manipulation go way beyond the cases of single acts of deceit. People, especially women and celebrities, are being exposed to unscrupulous modifications of their images, mostly against their will, and with few ways to get immediate redress. On a social level, fake videos and audio messages can trigger communal conflict and manipulate the election process as well as damage the reputation of governmental bodies. The implications of such technology being abused in a multi-ethnic and politically volatile nation such as India can extend to affect the social peace and constitutional governance far and wide.

Even though the current legal system in India, which incorporates provisions in the information technology laws, criminal laws and data protection principles offer certain actions, they have been thought of in a different technological age. They were not meant to cater to advanced and fast-changing nature of AI-generated synthetic media. The problem of establishing liability, the rate of content distribution, cross-border jurisdiction and platform accountability also demonstrate that the current regulatory framework has numerous weaknesses. This as it is law is frequently responsive to harm, not anticipatory of harm or even responsive towards harm. The challenges cannot be addressed by making the small adjustments. A holistic and proactive strategy is required that embraces lawmakers, technologists, Internet platforms, civil society and the courts. At the same time, the public should be provided with their avenues for legal recourse so that they can have a chance to remove, compensate and protect their reputation and dignity as quickly as possible.

We need to encourage the improvement of digital literacy and ethical technological development. Without the public awareness and ethical development of technologies, the regulatory improvements cannot be sufficient to safeguard democratic principles. Our constitutional rights should be the centre of the legislative efforts including the right of privacy, of freedom of expression and of reputation. Unless the issues are addressed in an urgent and explicit way, the damage cannot be only on individual but also on whole collective society, which is the foundation of democracy. Credibility of information, reliable security of the digital environment and credibility of the constitutional institutions rest in a legal and policy regime

that can respond to the emerging threats of technologies. In a rapidly changing digital world, It is mandatorily required to protect the rule of law through truth and accountability.