The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

REGULATING DEEPFAKES IN INDIA: EVALUTING THE ADEQUACY OF EXISTING LEGAL FRAMEWORKS

~ ***Trupti Hogade***

ABSTRACT

Artificial intelligence (AI) has transformed digital communications by making possible the creation of incredibly realistic synthetic media known as deepfakes. This is done through the application of machine learning techniques, specifically deep learning techniques, which are used to manipulate or produce audio, video, and images that look real. Despite the fact that there are many legitimate applications of this technology in the fields of entertainment, education, accessibility, and content creation, misuse of deepfakes has raised serious ethical and legal concerns. Deepfakes have increasingly been used for identity theft, fraud, disinformation, deception, blackmailing, and character assassination.

This paper analyses the concept of deepfake technology and examines the legal problems surrounding the creation and dissemination of deepfakes. The paper reviews the relevancy of laws existing in India concerning the problem, such as the IT Act of 2000, the Bharatiya Nyaya Sanhita of 2023, the Copyright Act of 1957, and the DPDP of 2023. Moreover, this paper juxtaposes the regulatory practices adopted in India against developments made in areas like the European Union, USA, and China. This paper argues that although the existing laws have little to offer in terms of resolving the problems caused by deepfakes, India is lacking an elaborate law on how to regulate artificial intelligence and synthetic media.

KEYWORDS: Deepfakes, Artificial Intelligence, Information Technology Act, Privacy, Cyber Law, Digital Regulation.

INTRODUCTION

Artificial intelligence (AI) is one of the most revolutionary technologies of the current century. The development of the technology known as deepfake has attracted many legal and regulatory concerns due to the capability of creating very convincing synthetic media. Deepfakes refer to digitally manipulated or artificially created audio, video, or imagery content using highly

advanced machine learning processes, making it hard to distinguish between fake and real content. The term 'deepfake' results from the combination of 'deep learning' and 'fake'. [1]

Deep learning technology is able to analyze big data sets and recreate facial expressions, speech, and body movements with impressive accuracy. [2]Therefore, individuals can be made to appear like they have done or said something which was never real. While the technology itself is not inherently malicious, the misuse of it presents serious ethical problems including privacy, reputation, democracy, and trust among others.[3] The increase in access to AI has made production of deepfakes easy. Many tasks which required highly sophisticated skills can nowadays be accomplished using software programs and online platforms which are publicly available.

The advent of deepfake technology in India has created fears for policymakers, regulators, and law practitioners.[4] The prevalence of instances of doctored videos has demonstrated how deepfakes may cause harm on many fronts such as economic, social, and psychological. Deepfakes may be used to commit fraud, identity theft, cybercrime, libel, and privacy invasion. They could also help spread misinformation.

Despite all of the aforementioned threats, there is currently no particular legal framework concerning deepfakes in India.[5] Legal responses, rather, are based on various laws created before the rapid increase in the use of synthetic content generated through AI technologies. Such issues raise serious questions concerning the effectiveness of laws in addressing challenges of deepfakes.

The present research seeks to evaluate the adequacy of the legal framework in place in India to control deepfakes. In the process, it will examine relevant legal statutes, reveal gaps in regulation, make comparisons to other countries, and propose recommendations for improvement.[6]

Understanding Deepfake Technology: Meaning, Evolution, Types, Benefits, and Risks

1. Meaning and Concept of Deepfakes

Deepfakes are artificial creations or modifications of media made through AI techniques such as deep learning and neural networks to create realistic but fake audio, video, images, or texts. The primary purpose of deepfake technology is to make a replication of an individual's appearance, sound, facial expressions, or actions in a way that makes the creation seem genuine.

1 Stuart J Russell and Peter Norvig, Artificial Intelligence: A Modern Approach (4th edn, Pearson 2021).
2 Robert Chesney and Danielle Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2019) 107 California Law Review 1753.
3 Nina Schick, Deepfakes: The Coming Infocalypse (Monoray 2020).
[4] Ajder Henry and others, *The State of Deepfakes: Landscape, Threats and Impact* (Deeptrace Report 2019).
[5] NITI Aayog, *National Strategy for Artificial Intelligence #AIForAll* (Government of India 2018).
[6] Ministry of Electronics and Information Technology (MeitY), Government of India, 'Advisory on Deepfakes and AI-Generated Content' (2023).

Deepfakes can be made through machine learning algorithms that are trained on large sets of images, videos, or audio of the target person. These systems learn patterns and characteristics of the target person and then make new content that imitates the real one. As the development of AI technology continues, it has become increasingly difficult to distinguish between the authentic content and the altered one.

The rapid development of deepfake technology has brought changes to the digital environment in terms of making highly realistic synthetic content. Even though there are a lot of beneficial applications of deepfake technology, its misuse has posed some serious concerns about privacy, cybersecurity, reputation, and democracy.

2. Evolution of Deepfake Technology

The emergence of deepfake technology may be traced back to the development of computer vision and machine learning technologies. Early approaches to image manipulation relied on manual manipulation through software programs like Adobe Photoshop. Nonetheless, such approaches required high technical proficiency and resulted in easily noticeable changes in most cases.

Deep learning algorithms have revolutionized the process of synthesizing media content. To be more precise, the invention of Generative Adversarial Networks (GANs) by the computer scientist Ian Goodfellow in 2014 enhanced dramatically the ability of artificial intelligence to create realistic-looking images and videos.[7] GANs are built around the interaction between two neural networks the generator and the discriminator to improve the quality of the generated content.

In 2017, deepfake technology gained popularity due to the emergence of communities online which utilized the capabilities of artificial intelligence to superimpose faces onto existing videos. Since then, technological advances have enabled the use of deepfake technology for more complex purposes, including real-time face swapping, voice impersonation, and AI-generated characters.[8] Nowadays, various software and mobile applications on the market allow even those who have no experience in manipulating media to create deepfakes within minutes.

3. Types of Deepfakes

Deepfakes are known to occur in different forms depending on the nature of content manipulated.

A. Face Swapping Deepfake

Face swapping refers to the substitution of a person's face with the face of another person in either the image or the video. Such type of manipulated content is commonly used for entertainment purposes but can also be applied maliciously.

---

[7] *Ian Goodfellow et al., Generative Adversarial Nets, in 27 ADVANCES IN NEURAL INFORMATION PROCESSING SYSTEMS 2672 (2014).*

[8] *UNESCO, Recommendation on the Ethics of Artificial Intelligence (2021).*.

B. Voice Clone Deepfake

Voice clone deepfake uses AI algorithms to generate voices of people from their audio clips that sound as similar as possible to the way particular people speak, including their accent and tone of voice.

C. Deepfakes with Lip Synchronization

Deepfakes with lip synchronization involve manipulating lip movement of a person in video by generating new audio clip that the person seems to have spoken.

D. Artificial Video Production

Through AI algorithms, it is possible to produce videos of synthetic personas who don't even exist. Such artificial content can be applied for good or bad purposes.

E. Images Created by AI

Through AI algorithms, lifelike images of people, objects and things can be generated that never existed. Such type of manipulated content can be applied artistically but also deceptively and fraudulently.

4. Legitimate Uses and Benefits of Deepfake Technology

Although commonly associated with cases of abuse, there are legitimate applications of deepfake technology.

A. Media & Entertainment

The film industry and other content providers can use deepfake technology in the creation of special effects, restoration of characters, voice dubbing, and recreations of history. The technology can reduce costs and increase creativity.

B. Education & Training

Educational institutions can create immersive learning experiences using AI-powered simulation and recreations of history. Deepfakes can help students visualize events from history and learn from virtual tutors.[9]

C. Accessibility & Communication

The voice synthesis technology can assist individuals with difficulties in speaking through the production of lifelike voices. The avatars powered by AI technology can also be used for multilingual communications and translations.

D. Business & Customer Relations

Companies increasingly use AI-powered virtual assistants and virtual presenters to facilitate client interactions and communication.

E. Preserving Cultural Heritage

Deepfake technology can help recreate historical characters and preserve cultural narratives.

5. Risks and Challenges Associated with Deepfakes

While they have many benefits, deepfakes pose several legal, ethical, and social problems.

A. False and Misleading Information

---

[9]*Danielle Keats Citron & Robert Chesney, Deep Fakes and the New Disinformation War, 95 FOREIGN AFFS. 147 (2019).*

[10]*nformation Technology Act, No. 21 of 2000, § 66C (India).*

[11] *Information Technology Act, No. 21 of 2000, § 66D (India).*

Deepfakes can be used to produce fabricated narratives and misleading data. Edited clips featuring people making false statements can influence public perception and undermine the credibility of sources of information.[10]

B. Privacy Issues

The unauthorized use of an individual's face, voice, or picture amounts to a violation of privacy rights. The individuals often face distress and reputational damage from the distribution of such material.[11]

C. Unwanted Intimate Images/Video

One of the major concerns associated with deepfakes is the production of intimate pictures/videos without consent. Such content especially affects women and raises many ethical concerns about consent and personal dignity.

D. Financial Scams and Identity Theft

With the help of voice duplication and manipulated media, one may easily resort to deception. Fraudsters can impersonate business executives, family members, and governmental officials to obtain some kind of profit.

E. Manipulation of Elections and Democracy.

The use of deepfakes can influence elections through the distribution of fake speeches, misleading endorsements, and propaganda. This would put the integrity of the election and the democratic process at risk.

F. Decline in Public Trust.

Due to the wide availability of deepfake technology, there is a phenomenon known as the "liar's dividend," where truth could be dismissed as lies. This could result in a decline in public trust on digital evidence.

6. Need for Legal Regulation

With the increasing complexity and availability of deepfake technology, it is becoming increasingly important to have stringent laws regulating deepfakes. Traditional legal systems may have been set up prior to the advent of artificial intelligence-based synthetic media and may not address the risks associated with deepfakes in an effective manner. Therefore, it is imperative to reconcile technology with privacy, reputation, law and order, and democracy.

The next section discusses the present legal framework in India and examines the effectiveness of such laws to address the issues related to deepfakes.

Existing Legal Framework Governing Deepfakes in India

1. Information Technology Act, 2000

The Information Technology Act, 2000 (IT Act) is the primary legislation governing cyberspace and electronic communication in India. The IT Act does not define deepfake but there are many sections within the Act that could apply in dealing with problems emanating from deepfakes.[12]

A. Section 66C - Identity Theft

---

[12] *Information Technology Act, No. 21 of 2000, §§ 67, 67A (India).*

[13] *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (India).*

[14] *Bharatiya Nyaya Sanhita, No. 45 of 2023 (India).*

Under Section 66C of the IT Act, any act of deceitful use of another person's electronic signature, passwords, or other distinguishing identification factors is punishable by law. Any deepfake that uses someone else for nefarious purposes can be considered an identity theft offense.[13]

B. Section 66D - Cheating by Personation

Clause 66D is concerned with penalizing cheating through impersonation using computer systems. Any fraud using voice imitations and artificial intelligence-driven impersonations designed to obtain financial gain or any other advantage could fall under this provision.[14]

C. Section 67 and Section 67A

These laws prohibit the dissemination and communication of obscene or sexually explicit content through electronic means. Sexual deepfake content as well as sexual content produced without consent is punishable by these laws.[15]

D. Intermediary Liability

Due diligence requirements for social media sites and other intermediaries have been provided by the 2021 Rules of Information Technology (Intermediary Guidelines and Digital Media Ethics Code). Social media sites could be compelled to remove any illegal content like harmful deepfakes upon receiving proper notification.[16]

2. Bharatiya Nyaya Sanhita, 2023

The Bharatiya Nyaya Sanhita (BNS), which is an Act after the Indian Penal Code, contains several provisions that could potentially be utilized to prosecute deepfake creators and disseminators.[17]

A. Defamation

Deepfakes of individuals in positions that are damaging to their reputation could result in criminal defamation cases. AI-generated content, if false, could have detrimental effects on one's personal and professional reputation.

B. Forgery and Fabrication

In the case of deepfakes made for the intention of causing harm, deception, or gain from illicit activities, there may be provision in law regarding forgery, counterfeiting of documents, and fraudulent representation.

C. Criminal Intimidation and Harassment

Intimidation, coercion, harassment, and extortion using deepfakes could fall under criminal liability provisions of the BNS.

3. Right to Privacy and Constitutional Protection

---

[15] *Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).*
[16] *Digital Personal Data Protection Act, No. 22 of 2023 (India).*
[17] *Copyright Act, No. 14 of 1957 (India).*
[18] *European Union Artificial Intelligence Act.*

The right to privacy under the constitution is now an important safeguard against any harmful deepfake.

In the case of Justice K.S. Puttaswamy v Union of India (2017), the Supreme Court of India recognized privacy as a fundamental right guaranteed under Article 21 of the Constitution. [18]Unauthorized creation and dissemination of deepfakes containing an individual's image, voice, or appearance would be considered as violations of informational privacy, dignity, and autonomy.

Deepfakes may interfere with an individual's ability to control their own information and identity and, therefore, may raise constitutional concerns regarding privacy and human dignity.

4. **Digital Personal Data Protection Act, 2023**

The Digital Personal Data Protection Act, 2023 (DPDP Act) provides a framework for dealing with digital personal data in India.

Deepfaking usually involves the collection and analysis of personal data in the form of images, videos, audio clips, and biometric characteristics. The issue of possible violation of data protection norms may arise when personal data is used without consent.

Although the DPDP Act does not cover the matter of deepfakes, it may provide indirect protection through the provisions on consent and lawful processing of personal data.[19]

5. **Copyright Act, 1957**

Deepfakes can also raise serious concerns regarding copyright.

Employing copyrighted photographs, movies, audio recordings, or artwork without the required consent to create deepfakes can be deemed as copyright infringement. Furthermore, performers' rights may be at stake when the digital reproduction of the performance occurs without any prior consent. Copyright protection is limited to creative expressions rather than the person's identity.[20]

6. **Limitations of Existing Laws**

Despite the fact that there are numerous legal actions that can be taken, the current laws in India face the following problems:

1.No legal definition of what constitutes deepfake.

2.No regulations dealing with the use of artificial intelligence to create such synthetic material.

3.Problems in identifying the anonymous creators.

4.Problems associated with jurisdiction in regard to cross-jurisdictional distribution.

5.Content removal and regulation.

6.Limited responsibility to disclose the AI-created material.

7.Inadequate compensation systems for victims.

8.It implies that the current laws provide only patchwork protection against dangers posed by deepfakes.

Critical Evaluation of the Adequacy of Existing Laws and Regulatory Gaps

[19]European Commission, *Proposal for Harmonised Rules on Artificial Intelligence*.
[20]Nat'l Conf. of State Legislatures, *Deepfake Legislation Tracker*.
[21]U.S. CONST. amend. I.

1. Lack of a Legal Definition for Deepfakes

An important drawback of the existing law is the lack of a legal definition for deepfakes. Neither the Information Technology Act, 2000 nor the Digital Personal Data Protection Act, 2023 offers a clear legal definition of synthetic media created with the help of artificial intelligence.[21] The lack of a legal term makes it difficult to understand what degree of protection should be provided to the victim of deepfakes and hampers the process of enforcing laws against such actions. Investigation agencies and courts often have to classify the actions related to deepfakes in terms of those that were not intended for them.

2. Reactive Rather Than Preventive Regulation

The present legislation of India focuses mostly on providing remedy once there is any harm. The remedy for defamation, obscenity, fraudulent activities, or invasion of privacy could be sought legally once a deepfake has been created and distributed. However, the deepfakes may be disseminated on digital media platforms very rapidly, causing irreparable reputational and psychological harm before any remedy could be found. Once the content has been widely disseminated, its complete eradication becomes extremely difficult. The present legal system, therefore, does not have any provision for preventive measures.[22]

3. Problems with Identification and Attribution

Since deepfakes are usually created in a clandestine manner through encryption, VPNs, and servers located overseas, identifying where the altered material comes from is not always easy.In fact, even if an illegal deepfake video has been detected, there may be obstacles for law enforcement in identifying those responsible because they can be outside India's territorial jurisdiction. This problem becomes evident in cases involving international social media and the globalization of synthetic media.This makes legal measures less effective because the offender cannot be identified or held accountable.

4.Inadequate Measures to Prevent Non-Consensual Deepfakes

The creation of non-consensual intimate deepfakes is one of the most harmful uses of AI-generated content. Existing regulations on obscenity and sexually explicit material provide some form of protection; however, such regulations have not been specifically designed for dealing with synthetic media. Victims often experience problems in the procedure, delays in removal of content, stigmatization, and difficulties in receiving compensation. Furthermore, legal regulations generally focus more on the material than the unauthorized digital use of someone's identity and likeness. Therefore, existing approaches may fall short when protecting the dignity and privacy that is violated through these deepfakes.

5. Limitations of Data Protection Legislation

The Digital Personal Data Protection Act of 2023 indirectly offers protection from the particular instances of deepfake creation involving access to personal data without consent.[23] Nonetheless, the law does not cover AI-generated content or biometric reproduction.The development of deepfakes may happen using publicly

---

[22]*Provisions on the Administration of Deep Synthesis Internet Information Services (China) (2022).*

[23]*Bharatiya Nyaya Sanhita, No. 45 of 2023, §§ 111, 318, 336, 356 (India).*

available images, video, and audio from the internet. In such cases, questions arise about consent, lawful processing, and liability due to the absence of any regulation covering this area.The absence of any laws addressing the use of training data for AI systems or biometric misuse reduces the effectiveness of existing data protection mechanisms.

6.Issues With Platform Accountability

The social media websites play an important role in the diffusion of deepfakes. While intermediary laws necessitate the practice of due diligence, uncertainties remain about the extent of liability that the platform faces with regard to disinformation and altered media created through artificial intelligence.[24] Content monitoring is often unable to detect deepfakes efficiently. Any delays in detecting and removing harmful content can increase the damage suffered by the victim to a considerable degree.Additionally, the platforms can have different moderation rules.

7.Threats to Democracies

There are risks posed by deepfakes to democracy and the process of voting. The edited footage can be used to spread false information, shape the perception of people, or discredit political contenders. Quick generation and distribution of the altered media pose issues to relevant regulators and electoral commissions. Existing laws regarding elections and cyber security may not be enough to deal with the emerging technology-driven disinformation practices.[25] Without protection, deepfakes could undermine confidence in democracies and elections.

8.The Question of the "Liar's Dividend"

One particular challenge arising out of the development of deepfake technology is known as the "liar's dividend" problem. With increasing familiarity with deepfakes, there is the possibility that people will view truthful information as fake. There is a risk posed to the court, investigations, journalism, and the general public population. If individuals are able to reasonably claim that such content has been faked using AI, then it loses its evidentiary weight.[26]

9.Need for an All-Inclusive Legislation

The above limitations show that there is still an incompleteness and indirectness in the protective nature of existing Indian laws when it comes to deepfake related harms. Even if laws relating to cyber crime, privacy, obscenity, defamation and data protection still play a significant role, there is no coherent regulatory framework for synthetic media.

An efficient legislative framework would provide:

1.Definition of deepfakes
2.Mandatory disclosure of AI-generated content
3.Effective prevention against non-consensual synthetic content
4.Clear standards of platform accountability
5.Prompt deletion of content
6.Recovery mechanisms for the victims

---

[24] *Information Technology Act, No. 21 of 2000, § 79 (India).*
[25] *Digital Personal Data Protection Act, No. 22 of 2023, §§ 4, 8 (India).*
[26] *Press Information Bureau, Gov't of India, Government Advisory on Deepfake Content (Nov. 2023).*

7.Appropriate sanctions for the amount of harm caused.

Comparative Analysis of International Regulatory Approaches

1. European Union

A. Risk-Based Regulatory Framework

The European Union has established itself as an influential regulator of AI globally. The EU uses a risk-based approach with the objective of bringing the development of technology into balance with the protection of fundamental rights.In the context of EU AI regulations, individual AI systems are classified according to the risks they pose. Applications with the ability to affect humans or to generate fake content are subject to more rigid transparency obligations.[27]

B. Transparency Obligations

Transparency with regard to content generated by AI is stressed in the EU. People should know whether they deal with AI systems or artificial content.This transparency obligation is meant to reduce fraudulent behavior and enable users to distinguish between natural and artificial content.[28]

C. Advantages and Disadvantages

The main benefit of the EU approach is its preventative nature. It seeks to address the causes of misinformation and manipulation through imposing transparency obligations before the damage occurs.Yet, opponents believe that compliance obligations may put heavy pressure on businesses and tech developers.

2. America

A. Regulation by Sector

Unlike the European Union, the United States still lacks comprehensive regulation in form of a federal law addressing deepfakes. The regulation occurs through state laws and existing legal doctrines.There are many states that have adopted laws regarding deepfakes associated with elections.[29]

B. Concerns about Freedom of Speech

Regulation of deepfakes in the United States is largely influenced by constitutional protection of freedom of speech through the First Amendment.It is necessary for legislators to balance efforts to curb misinformation with constitutional problems connected to censorship and free speech.[30]

C. Pros and Cons

U.S. approach promotes innovations and avoids unnecessary regulation. However, the absence of a coordinated system in the country results in inconsistency in regulations between different states.

3. China

A. Mandatory Labeling Requirements

One of the most stringent approaches to regulating synthetic media has been adopted by China. The services provider of deep synthesis shall label content

---

[27] *Ministry of Electronics & Information Technology, Gov't of India, Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.*

[28] *UNESCO, Recommendation on the Ethics of Artificial Intelligence (2021).*

[29] *Organisation for Economic Co-operation and Development (OECD), OECD Principles on Artificial Intelligence (2019).*

[30] *European Parliament & Council, Regulation (EU) 2024/1689 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), 2024 O.J. (L).*

created using artificial intelligence.Due to this approach, it will be easy to avoid any form of deceit.[31]

B. Responsibility of the Platform

There is a heavy burden on technological firms as well as the platform according to the Chinese law. The providers of the service have to undertake verification and management procedures against illegal synthetic media.[32]

C. Regulatory Oversight

Regulation of synthetic media in China focuses heavily on government supervision. There is heavy power at the hands of officials to ensure compliance.

D. Strengths and Weaknesses

There are fast and efficient implementations with the adoption of this strategy in China. However, there are some concerns about freedom of expression and individual autonomy.

4. Lessons Learned for India

A comparison of various strategies across the globe has helped identify several valuable lessons for India.First, India may benefit from creating a legal definition of deepfakes consistent with evolving global practices.Second, requirements for transparency to disclose AI-created content can help reduce the risk of deception and disinformation.Third, accountability of platforms should be improved to ensure quick identification and removal of harmful synthetic media content.Fourth, special rules dealing with non-consensual intimate deepfakes can provide better safeguards for victims.Lastly, any regulatory framework should strike a balance between innovation, privacy, freedom of speech, and security.

5. Comparative Analysis

The EU values mostly transparency and risk control. The US relies upon a decentralized system based on constitutional protection of freedom of expression. China emphasizes tough regulation, mandatory labeling, and accountability of the platform.

All these models bring their strengths and highlight the respective priorities. India should not be tempted to adopt one of them uncritically but rather devise the system suitable for its constitutional framework, technological environment, and regulation needs.

Recommendations and Proposed Legal Reforms

A. Implementation of Laws on Deepfakes and Synthetic Media

The first thing to do is enact laws aimed directly at deepfakes and synthetic media. The relevant laws should:

1.A proper definition of deepfakes and other forms of synthetic media
2.Classify different types of synthetic media
3.Distinguish the legal and illegal uses
4.Set out the civil and criminal liabilities
5.Provide for proper implementation measures and sanctions.

---

[31] *Council of Europe, Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (2024).*

[32] *NITI Aayog, National Strategy for Artificial Intelligence: #AIForAll (Gov't of India 2018).*

B. Mandatory Disclosure and Labeling Requirements

India should consider implementing mandatory requirements for disclosing that the content is made by means of AI technologies.[33]

Automatic labeling of artificial content would serve as:

1.Promoting transparency
2.Reducing deception
3.Allowing users to make informed decisions
4.Allowing to recognize the altered content.

Mandatory requirements would become particularly important when it comes to political advertising, public communications, and dissemination of information.

C. Improving Platform Accountability

Social media platforms play an important role in the creation of deepfakes and therefore should be held accountable in ensuring they are not used inappropriately.[34]

Regulatory changes may include:

1.Fast removal procedures
2.Detection systems for AI-generated content
3.Transparency reports
4.Grievance procedures for users
5.Better cooperation with law enforcement.

Platforms that know about malicious deepfakes but fail to remove them in time should face consequences from regulations.

D. Better Protection from Unauthorized Deepfakes

Protection measures should be put in place to safeguard the affected people from unauthorized intimate deepfakes.[35]

Legislation should ensure that:

1.Making production and distribution of this kind of content illegal
2.Rapid process of deportation
3.Privacy of victims should be maintained
4.Victims should be compensated for their loss
5.Reporting mechanism should be provided.

E. Relation to Data Protection Legislation

The Digital Personal Data Protection Act, 2023 requires further amendments addressing biometric and identity information used by AI applications.

This can be achieved by including:

1.Consent requirements for the use of facial imagery and audio
2.Restrictions on the use of unauthorized biometric information replication

---

[33] *World Economic Forum, The Global Risks Report 2024 (19th ed. 2024).*

[34] *Danielle Keats Citron, The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age (W.W. Norton & Co. 2022).*

[35] *Sam Gregory, Preparing for the Age of Deepfakes and Synthetic Media, WITNESS (2019).*

3.Transparency requirements regarding the datasets being used for AI training
4. Accountability measures for organizations processing personal information in the development of AI systems.
This will go a long way in preventing the abuse of personal information in the production of deepfakes.

F. Protection of Election Communication

The protection of communication regarding elections should take into account the potential effects of deepfakes in democracy, and thus certain protective measures need to be put in place during election periods.
These protective measures could include:
1.Compulsory notification of politically motivated content generated through AI technologies
2.More expedient process for reviewing deepfake election content
3.Greater powers for the election authorities
4.Repercussions for intentionally distributing misleading political synthetic media.

G. Awareness Among the General Public and Digital Literacy

Legislations alone can never take away the risks posed by deepfakes. Public awareness and digital literacy are both essential components of an effective regulatory strategy.
It is important for government agencies, educational establishments, and community groups to work in tandem for:
1.The education of the general public on the existence of deepfakes
2.The promotion of media literacy
3.Good online behavior
4.Improved capability to detect manipulated information.
Knowledgeable individuals can be considered an effective armor against misinformation.

H. Financing Detection Technologies

The government of India must encourage research and development into technologies that can detect deepfake videos.
This can be done through:
1.Financing research projects;Academic collaboration
2.Public-private sector collaboration
3.Incentivizing technological innovation among developers.
Higher levels of detection will aid in the identification of such synthetic media on platforms, by law enforcement, and in court proceedings.

I. International Cooperation

Deepfake videos frequently cross international boundaries, thereby requiring international cooperation.It is necessary for India to step up its international

cooperation efforts with foreign governments, international organizations, and technology companies in areas such as[36]:

1.Information dissemination
2.Analysis of transnational crimes
3.Standardization of regulations
4.Strategies regarding the regulation of synthetic media.

Conclusion

One of the main issues arising due to rapid development of AI is related to deepfakes technology. It has changed the nature of digital information as it is now possible to create highly realistic synthetic audio, video, and images. Even though there are many positive aspects of this technology for entertainment, education, accessibility, and communication, misuse of deepfakes has caused serious problems concerning privacy, reputation, cybersecurity, misinformation, fraudulent activities, and even threats to democracy. This study investigated the issue of deepfakes technology and focused on its uses and threats. In fact, it was found that deepfakes can cause serious harm through impersonation, non-consensual explicit content, identity theft, politics, and misinformation. As far as artificial intelligence is developing rapidly, it becomes harder to distinguish authentic content from fake, hence, the necessity of appropriate regulations arises.

The study further analyzed the prevailing legal system in India that includes The Information Technology Act, 2000, Bharatiya Nyaya Sanhita, 2023, Digital Personal Data Protection Act, 2023, rights to privacy provided under the constitution, and copyright law. While there may be some ways through which such laws can provide compensation to people for the harm caused due to deepfake technology, these laws have not been enacted to control AI generated synthesized content. Therefore, the current legal system remains fragmented and insufficient to address the problems posed by emerging technologies.

In this regard, a number of weaknesses in existing laws were pointed out including no definition of deepfakes in law, difficulties in identifying anonymous violators, lack of adequate defenses against non-consensual creation of synthetic media, unclear issue of platform responsibility, and absence of safeguards against AI-generated disinformation. Such findings mean that current legislative framework provides rather limited protection and can find it difficult to counter new forms of digital manipulation.

Comparative analysis of the regulatory approaches implemented by EU, USA, and China showed that states around the world actively develop regulatory approaches to combat the dangers associated with synthetic media. Despite the fact that different methods of regulation are used in these jurisdictions, certain common trends emerge including transparency, platform responsibility,

[36] *Robert Chesney & Danielle Keats Citron, Deep Fakes and the New Disinformation War, 95 FOREIGN AFFS. 147 (2019).*

disclosure, and greater protection from potential misuse of AI technology. All these innovations have valuable lessons for future regulations in India.

This study highlights that even though there are certain legal ways to address injuries caused by deepfakes under existing laws of India, these laws do not offer sufficient measures for regulating synthetic media created with the help of AI technology. There is a need for an active and focused legal policy for dealing with deepfake technology which poses many challenges due to its rising popularity and increasing complexity. An advanced regulatory framework based on law, technology, oversight, and public awareness needs to be developed.

With the development of artificial intelligence changing the contemporary world, one should pay attention to the necessity of legal means for making technological developments serve the interests of people. The issue of regulating deepfakes is part of this problem.