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

DEEPFAKE REGULATIONS IN INDIA: LEGAL CHALLENGES TO PRIVACY, CONSENT AND DEMOCRACY

-Atulya Srivastava

ABSTRACT

Deepfake technology poses serious threats to law and society in India due to the rapid emergence of artificial intelligence and digital platforms. Deepfakes refer to audio, video or images generated through AI that may be used to impersonate people without their consent. Though there are several legitimate applications of deepfakes for use in entertainment or educational purposes, their abuse poses serious issues in areas such as privacy, identity theft, misinformation, and democratic processes. There have been many cases of deepfakes being used in India for pornography, political manipulation, financial scams, and cyberbullying, especially against women and celebrities. Though there have been some provisions made under the existing laws like the Information Technology Act of 2000 and the Bharatiya Nyaya Sanhita 2023, there are no laws to deal specifically with deepfakes. This paper will explore the legal challenges associated with the phenomenon of deepfakes with regard to issues of privacy, consent, and democracy in India.

KEYWORDS

Deepfake Technology, Artificial Intelligence, Privacy, Consent, Democracy, Synthetic Media, IT Act 2000, Digital Rights

INTRODUCTION

The rise of artificial intelligence has drastically changed how we experience the modern digital landscape as machines can increasingly imitate human behavior. One of the most controversial aspects of this technology is how deepfake has developed over the last several years, because it uses digitally-manipulated content—both audio, video, and still images—that was created using artificial intelligence technologies but can now also accurately simulate an individual speaking or acting in a way that they have never done so before.[1] In fact, the term 'deepfake' comes from the terms 'deep learning' (a type of machine learning technology) and 'fake' in general. To create deepfakes, artificial intelligence typically uses a form of neural networks and generative adversarial networks to produce synthetic content.[2]

While deepfake technologies gained initial-public exposure from entertainment and experimental uses across the social media platforms, they have quickly evolved into a global-legal and political-problem based upon their misuse in unsafe, non-consensual ways. Examples of misuse include the following: the creation of non-consensual pornography, fraud perpetrated through the abuse of trust using impersonation, misinformation dissemination and defamation.[3] In democratic societies, the complexity and severity of these problems has an especially detrimental effect when you take into consideration that a significant portion of the environment where public discussion occurs is fully-digital (digital communication/media, electronically-based social platforms, etc.).

---

1. Robert Chesney & Danielle Citron, Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, 107 Calif. L. Rev. 1753 (2019)
2. . Id.
3. Danielle Keats Citron, Sexual Privacy, 128 Yale L.J. 1870 (2019).

The environment for generating deepfakes is extraordinarily conducive within India as a result of a significant increase in the use of the Internet, as well as social media, multiple languages, and low levels of digital literacy that exist throughout India. Manipulated political speeches (from leaders and those running for office), phony sources of entertainment, and non-consensual pornography are already examples of how much work can be done through the use of deepfakes to weaken social stability and destroy trust in one another.[4]

In addition, many women are victims of non-consensual pornography through deepfakes which continues to amplify issues around the consent and dignity of individuals.[5]

What makes this situation even more difficult is that there is no law addressing deepfakes within India. Most of the existing statutes were passed prior to the development of the new forms of synthetic media and as such, the courts and other enforcement agencies responsible for enforcing the statutes have to use multiple statutes (fragmentation) concerning obscenity, impersonation, defamation, identity theft, cybercrime, and various violations of privacy.[6] These existing legal rights can often fail to meet the current advancements in technology with the use of AI generated identity duplications and misinformation generated by robot-generated systems.

In addition, deepfakes raise constitutional tensions as well. The right to free expression (under Article 19(1)(a)) is intended to protect artistic expression and political expression; on the other hand, the right to privacy and dignity (under Article 21) protects individuals from being exploited for profit, or otherwise.[7] The dilemma for any one person is finding a proper balance between technological advancement and expression versus the harm to society caused by malicious synthetic media. In addition, the use of manipulated political content also raises concerns relating to the transparency of the electoral process by the influence of voters in making their electoral decisions and ultimately threatens the functioning of our democracy.

---

4. Ministry of Electronics and Information Technology, Advisory on Deepfake Misuse and Online Harm (2023)
5. Henry Ajder et al., The State of Deepfakes: Landscape, Threats, and Impact (Deeptrace Labs 2019).
6. Information Technology Act, No. 21 of 2000, §§ 66C, 66D, 66E, 67, 67A, India Code (2000).
7. INDIA CONST. arts. 19, 21.

The research paper explores the implications of the growing problem of deepfakes in India in terms of privacy rights, consent and the effect of deepfake technology on democratic values. There is also an analysis of the current legal framework with respect to deepfakes in India, its weaknesses, the use of similar frameworks internationally, and suggestions for new laws to cover the issue of deepfakes in Indian legislation.

UNDERSTANDING DEEPFAKE TECHNOLOGY

Artificial Intelligence (AI) approaches such as machine learning and deep neural networks are used to produce deepfakes. Generative adversarial networks (GANs) train one neural network to generate synthetic images/videos, while having a 2nd neural network attempt to detect image/video manipulations.[8] The generator improves its ability to create realistic content until the synthetic content is virtually indistinguishable from real."

Face swapping, voice cloning, altering someone's lip movements to match new speech, and creating a completely new persona in a video are all examples of deepfake technology. Many recent AI technologies allow for great accuracy in replicating an individual's voice, facial expressions, gestures and speech patterns. Access to many open-source AI programs, along with the use of cloud computing, has made creating deepfakes much less complicated from a technical perspective.[9]

While deepfake technology isn't illegal in itself, they can be used for legitimate purposes such as film/media, video games, accessibility tools, translation, historical recreation, satire and education. In fact, the negative uses for deepfake technology have progressed much more quickly than government regulation has been able to keep up.

---

8. Ian Goodfellow et al., Generative Adversarial Nets, 27 Advances in Neural Information Processing Systems 2672 (2014).
9. Sam Gregory, Deepfakes and the Future of Truth, 35 Witness Media Lab Rep. 1 (2020).

The most worrying negative uses of deepfakes include:

- Non consensual sexual content
- Political misinformation
- Financial fraud and impersonation
- Defamation and reputational attacks
- Synthetic evidence in legal disputes
- Cyber extortion and blackmail

The viral nature of social media further amplifies these harms. Once deepfake content spreads online, removing it completely becomes nearly impossible. Victims often suffer irreversible reputational and psychological damage before legal remedies can be obtained.

Additionally, researchers have called this the "liar's dividend,"[10] because someone who is accused or incriminated by reliable evidence may use AI-generated content to technically lie about the validity of the evidence. Therefore, deepfakes can erode the level of credibility and trust in legitimate information and falsified information, making the lack of information credibility one of the biggest threats to democratic societies.

DEEPFAKE AND RIGHT TO PRIVACY

The Supreme Court of India in Justice K.S. Puttaswamy v. Union of India,[11] held that to have an individual's right to privacy established by those with a vested interest, there must be a provision relating to that individual's constitutional right. Privacy is acknowledged by the law in a constitutional sense as a fundamental right established under Section 21 of the Constitution. The three separate and distinct ways in which privacy can exist are:

(1) informational privacy;

(2) bodily autonomy;

(3) decisional privacy.

10. Robert Chesney & Danielle Citron, supra note 1.
11. Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.

Each of these types of privacy is considered a necessary part of the value of privacy that is enshrined in the Constitution.

The use of deepfakes violates both informational and personal privacy because deepfakes allow for the manipulation of an individual's likeness, identity, voice, and appearance without their consent. A person's face and voice are two highly personal characteristics that carry a person's dignity and autonomy. When an AI uses deepfakes to mimic an individual's characteristics without their consent, that is an infringement upon an individual's personal identity.

As to the multi-faceted privacy harm from deepfakes, first, deepfakes deprive individuals of the right to control their digital identity; second, the presence of deceitful content may expose an individual to public humiliation or harassment; and third, the use of deceitful media may result in an individual being connected inappropriately to criminal, sexual, or immoral conduct. Additionally, women, journalists, activists, and public figures have an increased susceptibility to deepfake-related privacy harms, as their digital identities are publicly available and therefore serve as a rich source of training data for AI systems.[12]

In this country, privacy breaches are legislatively addressed through many different laws that do not connect with each other. For example, the information technology law makes it a crime to record or transmit a person's private image without their permission (section 66E)[13] or to publish obscenity and sexual material electronically (sections 67 and 67A).[14] In addition to those laws, other various sections of the Bharatiya Nyaya Sanhita, 2023,[15] criminalise offences such as identity theft, forgery, obscenity, and defamation. However, none of these laws were designed specifically for addressing and penalising acts of synthetic media manipulation.

---

12. Danielle Keats Citron & Mary Anne Franks, Criminalizing Revenge Porn, 49 Wake Forest L. Rev. 345 (2014).
13. Information Technology Act § 66E.
14. Id. §§ 67, 67A.
15. Bharatiya Nyaya Sanhita, No. 45 of 2023, §§ 294, 336, 356.

One of the major weaknesses of Indian law is that it focuses on the publication stage of provably deepfaked content and not on the production stage. Thus, an individual who has been digitally cloned may have experienced some levels of harm before they experience the harm that occurs when their clone is disseminated to the public at large. Current laws do not address the creation of AI generated voice clones and / or the creation of AI impersonations either.

Another challenge is enforcement. Since deepfakes can be circulated via encrypted platforms and hosted on remote servers, the challenge of having jurisdiction over them combined with the lengthy process of having them removed often makes legal recourse ineffective. Additionally, victims of deepfakes may not be able to identify an anonymous creator, and may not be able to obtain a prompt injunction to stop distribution of the deepfake.

Concerns have been heightened due to a lack of a complete system for protecting personal data. Although the Digital Personal Data Protection Act, 2023 has been passed into law, biometric manipulation and the creation of synthetic identities continue to fall outside the scope of the legislation's regulatory authority.[16] In developing fake images (i.e., deepfakes) through the use of both facial and voice samples,, the issue of informed consent is particularly pertinent; as is whether a second party may utilise data created through this process.

Deepfakes expose the inadequacies of the current privacy laws in India. The Constitution's right to privacy cannot sufficiently protect against advanced technological threats without adequate statutory protections.

CONSENT AND DIGITAL AUTONOMY

Lawful digital interaction rests on the concept of consent. Deepfakes destroy consent by allowing third parties to manipulate a person's image without the individual’s permission. When no consent exists, synthetic media is a significant breach of both autonomy and dignity.

16. Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).

The issue is particularly bad with non-consensual intimate deepfakes. Research indicates that the vast majority of Deepfake pornographic content has been created to target women.[17] Such material can destroy someone's reputation; inflict psychological damage; hurt their ability to work; and cause them to be harassed online.

Indian law inadequately addresses this phenomenon. Sections 67 and 67A of the Information Technology Act criminalise obscene and sexually explicit electronic material, while the Bharatiya Nyaya Sanhita penalises voyeurism and obscenity.[18] However, these laws do not explicitly recognise synthetic sexual imagery created through AI manipulation

The harms of consent extend beyond those related to pornography. Scammers are increasingly using AI-generated speech as a method to create fake voices (voice cloning) of others without their consent (e.g. family members, corporate executives, or public officials). By taking advantage of the emotional connection between their victims and the person who is being impersonated, scammers are able to trick their victims into sending them money or providing them with private information. Laws regarding fraud do not currently address the issues presented by AI-based fraud, including deception through synthetic identities.

One area of significant concern is informed consent for the purpose of collecting data. AI requires many datasets in order to develop AI products (such as images, audio[sound files], and video[s]). Many tech companies collect data by scraping publicly available content from websites without first obtaining users' authorization/permission.[19] Many individuals do not know that images of themselves and/or audio/video recordings are collected to develop generative AI systems that may mimic their likeness/identity.

17. Henry Ajder et al., supra note 5.
18. Information Technology Act §§ 67, 67A
19. European Data Protection Board, Guidelines on Consent Under Regulation 2016/679 (2020).

.

Other related questions with broader implications involve the ownership of identity attributes. There is currently no clear legal context in India that defines an individual's "personality rights", which would give an individual claims to ownership of his/her image and likeness. While the courts in India have recognised an individual's personality rights in the past (mostly concerning celebrities), there is not a developed body of jurisprudence.[20] Therefore, there are virtually no protections for common people.

The difficulty goes beyond the misappropriation of property, and concerns whether a person should have a legal right to control the reproduction (or digital reproduction) of his/her likeness or identity. If no strong laws are in effect concerning consent to use someone's likeness, there is a risk that it will become common practice to use this technology to use an individual's likeness against him/her.

DEEPFAKE TECHNOLOGY AND DEMOCRACY

Because deepfake technology has the potential to degrade the three pillars of democracy:
1) an informed electorate,
2) a transparent election process, and
3) trust in the source of information about the government,
The use of this technology presents an immeasurable threat to democracy. All three of these pillars are infracted by deepfake technology.

Deepfakes could mislead and ultimately give false information to voters through manipulated speeches, false campaign ads, and a fraudulent purpose. By creating digitally manipulated content, deepfake technology is capable of creating a propaganda-style advertisement that plays to voters' emotions, communal divisions, and political bias. During an election campaign, false information is quickly disseminated through social media and is often consumed by users in the form of short-form videos without sufficient verification.[21]

---

20. Anil Kapoor v. Simply Life India, CS(COMM) 652/2023 (Del. HC Sept. 20, 2023).
21. Claire Wardle & Hossein Derakhshan, Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making, Council of Europe Report DGI(2017)09.

India is particularly at risk in its digital environment because of the size of the population that uses social media daily and the high number of people using encrypted messaging platforms. The potential for regional or local-level suppression of deepfake material that is produced in different languages will expand exponentially over the next year, allowing a deepfake to reach millions of individuals in a matter of hours.. The combination of low digital literacy levels among the population and confirmation bias will make consumers of digital media extremely vulnerable to consuming manipulated digital content.

Using deep fake technology, many types of false news can be created, including digitally manipulated speeches by politicians. Also, false riot can be created, fake military announcements can be created, fake acts of violence between different communities can be created, and fake inflammatory comments can be produced by political leaders. All of these types of false media could cause panic, create social unrest, or cause an international conflict to happen before the false information can be verified by credible sources.

Trust in democracy is in jeopardy as a result of misinformation and lack of clarity. When people receive fake information from both traditional media outlets (e.g., television) and non-traditional media sources (e.g., social media), their trust in journalism, government communication and electoral information can be eroded. The so-called 'liar's dividend' is that politicians and public figures can ignore legitimate evidence with the excuse that it is fakes, thereby eliminating accountability mechanisms.[22]

Current Indian electoral laws do not have the tools to combat AI-generated misinformation, even though there are laws regulating electoral misconduct and corrupt practices as set forth in the Representation of the People Act of 1951.[23] The Indian Election Commission also lacks the specific statutory authority to regulate AI-created political content.

22. Robert Chesney & Danielle Citron, supra note 1.
23. Representation of the People Act, No. 43 of 1951, India Code (1951).

Intermediaries have some obligations as a result of the recent issuance of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021;[24] however, moderation practices of the platforms are largely inconsistent and reactive to incidents. Automated detection systems are also inadequate at identifying sophisticated deepfakes, particularly if the deepfakes are created in regional languages as is often the case.

As countries deal with the highly detrimental effects of misinformation produced by deepfake media not only in the election but also against the broad scope of government, the potential impact of such campaigns clearly indicates that the use of deepfake media to affect election outcomes will occur in India at some point.[25] Given India's geopolitical position and its extensive social diversity, it is sufficient to expect coordinated disinformation campaigns using synthetic media to happen in India

Ultimately, there are many ways to protect the integrity of democracy (criminal) but first and foremost there needs to be institutional support for democracy through proactive measures to safeguard elections (i.e., committees), platform accountability (i.e., regulations), and rapid verification mechanisms.

CURRENT LEGAL FRAMEWORK IN INDIA

At present, deepfake-related harms in India are governed by an assortment of relevant constitutional principles, applicable criminal statutes, relevant cyber regulations, and related intermediary obligations.

24. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Gazette of India, Extraordinary, pt. II sec. 3(i) (Feb. 25, 2021).
25. European Parliamentary Research Service, Tackling Deepfakes in European Policy (2021).

A. CONSTITUTIONAL PROTECTION

Various constitutional protections relate to privacy, dignity and personal liberty under Article 21 of the Constitution. The Supreme Court affirmed privacy as a fundamental right in its ruling in Justice K.S. Puttaswamy v. Union of India.[26] As such, deepfakes that alter how one's identity (including by creating fake images) might violate one's constitutional rights by subjecting one to humiliation or similar forms of harm. Article 19(1)(a) protects freedom of speech and expression, but any regulation concerning deepfakes must strike a balance between the interest of the general public to prevent a violation of free expression against the potential for the violation of one's constitutional rights through the use of deepfakes.[27]

B. INFORMATION TECHNOLOGY ACT, 2000

The Information Technology Act remains India's principal cyber law statute. Several provisions may apply to deepfakes:

1. Section 66C addresses identity theft.[28]
2. Section 66D criminalises cheating through impersonation using computer resources.[29]
3. Section 66E penalises privacy violations.[30]
4. Sections 67 and 67A prohibit obscene and sexually explicit electronic content.[31]
5. Section 69A gives special authority to take down online content when all required parameters have been satisfied.[32]

However, many of the provisions remain technologically outdated (e.g., deepfake videos, synthetic media and biometrically manipulated or AI-generated identities are not defined in the law).

---

26. Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
27. INDIA CONST. art. 19(2).
28. Information Technology Act § 66C.
29. Id. § 66D.
30. Id. § 66E.
31. Id. §§ 67, 67A.
32. Id. § 69A.

C. BHARTIYA NYAYA SANHITA2023

The Indian Penal Code has been replaced with the Bharatiya Nyaya Sanhita, which has sections for forgery, defamation, obscenity, impersonation and cyber-enabled offences.[33] These provisions may cover issues related to malicious deepfakes, but the Act does not contain any definitions specifically related to artificial intelligence or provisions for enforcement.

D. COPYRIGHT AND PERSONALITY RIGHTS

Copyright law can protect the manipulation of audiovisual works; however, copyright exists in the creator and not in the person appearing in the work. If a person has been manipulated in a work, they will only have limited rights to protection unless they own the material used in the manipulated work.[34]

Although both Anil Kapoor and Amitabh Bachchan have used their rights of personality in Indian courts, few citizens have had the opportunity to use the courts to claim their rights of personality due to the lack of widely available judicial recognition.[35]

E. RULES FOR THE INTERMEDIATION

Under the Information Technology Act, 2022, intermediaries have a requirement to follow due diligence and eliminate illegal content on notification.[36] Social media intermediaries that meet certain criteria as identified by the Committee must have a grievance officer designated, and comply with the obligation to take down material when notified..

Enforcement of the above continues to be inconsistent. Often, social media platforms will only operate their take-down process after being pressured publicly to do so. Further, automated moderation software continues to be incapable of consistently identifying or removing high-quality and nuanced synthetic media.

---

33. Bharatiya Nyaya Sanhita §§ 294, 336, 356.

34. Copyright Act, No. 14 of 1957, India Code (1957).

35. Amitabh Bachchan v. Rajat Nagi, CS(COMM) 819/2022 (Del. HC Nov. 25, 2022).

36. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

INTERNATIONAL PERSPECTIVE COMPARATIVELY

Different countries have implemented specific regulations related to deepfakes.

1. IN THE UNITED STATES OF AMERICA

The American legal system is decentralized; therefore, states have passed Anti-Deepfake legislation. California and Texas have passed laws prohibiting the use of synthetic video technology to create deepfake videos for political purposes or for sexually explicit material without consent.[37]

On the federal level, there have been proposals to regulate AI-generated impersonation and misinformation during elections. However, asa result of strong First Amendment protections against restrictions on political speech or satire, U.S. courts are very apprehensive in imposing restrictions on the use of deepfake technology.

2. IN THE EUROPEAN UNION

The European Union has developed a multi-prong strategy for regulating the use of deepfake technology through the proposed AI Act and the Digital Services Act.[38] Key regulations include the mandatory labelling of synthetic content (deepfake video), mandated transparency of synthetic content due to the obligation for providers that deploy synthetic content to assume liability, and a risk classification system that categorizes different types of synthetic content from a lowrisk to highrisk basis.

The General Data Protection Regulation also provides strong protections regarding biometric data and informed consent.[39]

---

37. CAL. ELEC. CODE § 20010 (West 2019).

38. European Parliament, Artificial Intelligence Act, EUR. PARL. DOC. PE-CONS 24/24 (2024).

39. Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016, 2016 O.J. (L 119) 1.

C. CHINA

China has enacted very strict regulations about deepfakes. All synthetically produced items must be labelled in a very clear way with COA (Certificate of Authorization). Also, all synthetically produced items must be labelled with the individual in question's written permission in order to be legal.[40] Thus, if one were to produce an item that was synthetically produced without obtaining their written permission, one can be held liable.

While the model of regulation in China demonstrates a lot of control via regulation, there are issues of censorship and surveillance from the government.

D. OPPORTUNITIES FOR INDIA TO LEARN

India cannot simply copy what is being done in other countries, as each country has its own unique constitution, social and technological attributes. Nevertheless, through the comparative model we can examine common principles.

1.Mandatory disclosure of synthetic media
2. Consent requirements for identity replication
3. Platform accountability mechanisms
4. Election specific safeguards
5. Rapid takedown procedures
6. Clear criminal liability for malicious use

India presently lacks each of these component in a coherent statutory framework.

REGULATORY CHALLENGES IN INDIA

India faces several structural and institutional challenges in regulating deepfakes.

---

40. Provisions on the Administration of Deep Synthesis Internet Information Services (China 2022).

A. TECHNICAL COMPLEXITY

The evolution of deepfake technology will continue to be faster than the speed of legislation. This puts in jeopardy the detection systems that are typically behind the generation capability; therefore, many advanced synthetic media could escape being automatically detected.

B JURISDICTIONAL CONFUSION

Often, creators of deepfakes remain anonymous and do so in a cross-border manner. Due to the location of platforms hosting the content (outside India), there are additional complications related to enforcement and collect evidence. The Indian police lack jurisdiction and authority to enforce laws against individuals who are located outside of India.

C. BALANCING FREE SPEECH

Excessively strict regulation can lead to the suppression of satire, parody, news, artistic expression and/or legitimate political speech. The ambiguity of the definitions within law could lead to increased levels of censorship and overreach by the government.

D. LACK OF ENFORCEMENT RESOURCES

The cybercrime units within the Indian government often lack the ability to dedicate resources to investigate and/or prosecute cases because of a lack of resources to investigate and a lack of personnel with AI expertise. As a result, investigation and prosecution of deepfake cases will not be effective due to the rapidity at which video deepfakes spread..

E. INCENTIVES FOR PLATFORMS

A social media company is potentially profiting economically from viral content. High-visibility viral content often has a lot of controversy, and therefore more advertisers are likely to advertise on a site that has high-visibility viral material. As such, platforms may not have a strong incentive to vigorously moderate harmful deepfake content.

F. PUBLIC KNOWLEDGE GAP

A large number of users cannot recognize altered media. A lack of digital literacy makes people more likely to fall victim to deceptive media and identity fraud.

These difficulties show that only using new laws to solve these issues is not enough. You need institutions with enough capacity, and technology investments, and educating the public to effectively regulate the business.

RECOMMENDATIONS AND REFORMS

India requires a specialised and rights oriented deepfake regulatory framework. The following reforms are necessary

A. ENACT DEDICATION LEGISLATION TO COMBAT DEEPFAKES

India must pass specific laws defining deepfakes and how they can be used. Distinctions must be made between synthetic media produced for malicious reasons and those produced for legitimate purposes such as art or education.

The definition must include:

- AI generated synthetic media
- Biometric replication
- Voice cloning
- Identity manipulation
- Non consensual synthetic content

B. REQUIRED DISCLOSURES

All AI-produced audiovisual works must have some form of either visible disclosure label or digital watermark. Including transparency in audiovisual quality would improve the perceived integrity of the information produced by malicious deepfake creators.

C. CRIME AND ABUSE

The law should criminalise:

- Non consensual intimate deepfakes
- Fraudulent impersonation
- Election related misinformation

- Synthetic extortion and blackmail
- Harmful identity manipulation

The penalties for any violations of these laws should be equal to the harm done, and have harsher penalties for repeat offenders and for distributing misinformation on an organised basis.

D. RIGHT TO PROTECT YOUR IDENTITY BASED ON YOUR CONSENT

People should have the right to control how their digital facial images, voices and likenesses are used. Companies must obtain publicly stated consent prior to using someone's biometric signature to generate synthetic media based on that person's identity.

E. INCREASING THE LIABILITY OF THIRD PARTIES

Platforms should implement:

- Rapid takedown mechanisms
- AI detection systems
- Verified reporting channels
- Transparency reports regarding synthetic media moderation

Failure to act upon clearly unlawful deepfake content should attract liability.

F. ELECTORAL SAFEGUARDS

The Election Commission of India should receive statutory authority to:

- Monitor AI generated election misinformation
- Order emergency takedowns
- Mandate disclosure for synthetic political advertisements
- Collaborate with platforms during elections

G. EDUCATING THE PUBLIC ON DIGITAL LITERACY

Regulating access to digital media requires a coordinated nationwide effort to increase public awareness and literacy, including training to help citizens identify manipulated content and how to verify source material.

H. TRAINING LAW ENFORCEMENT

Judges, police officers, prosecutors and forensic experts must be specially trained on how to evaluate AI-generated evidence and detect fake or synthetic media.

CONCLUSION

Indeed, deepfakes constitute one of the most significant legal and democratic dilemmas facing the world today in light of developments in the field of artificial intelligence. While there exist legitimate uses for the technology and artificial media in general, the use of such technology poses numerous problems with respect to privacy, consent, dignity, trust in public discourse, and democracy itself. Currently, Indian law offers no comprehensive protection against deepfakes, although several relevant laws do exist..

Specifically, it is worth mentioning that the Constitution of India recognizes the right to privacy as implicit in Article 21. However, in light of contemporary legal challenges, such a right is insufficient to guarantee adequate legal protection. Indeed, deepfakes have exposed several key flaws in India's current legal structure, including intermediary liability, biometric consent, electoral integrity, and digital governance.

As a matter of fact, India needs a new regulatory strategy with regard to deepfakes, which is both constitutional and democratic at the same time. Over-regulation is just as problematic as non-regulation in this context since it carries with it excessive censorship and restrictions on speech, while lack of regulation enables misuse of the technology and disinformation.

In the end, the governance of deepfakes is not merely a question of regulating artificial intelligence. Instead, it’s about maintaining human agency, truth, and constitutional democracy in a world where reality can be synthetically fabricated.