IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

DEEPFAKE TECHNOLOGY AND UNFAIR TRADE PRACTICES: A REGULATORY VACCUM IN BUSINESS LAW

Dr. Bhawna Singh Baghel

Assistant Professor

School Of Law, PIMR (Deemed To Be University), Indore

Dr. Sneha Singh

Assistant Professor

School Of Law, PIMR (Deemed To Be University), Indore

ABSTRACT

Deepfakes are an emerging form of artificial intelligence that is transforming digital communication and media production. They offer several benefits, including creating entertainment content, improving film production through digital characters, and supporting healthcare by assisting doctors in communicating with remote patients. At the same time, deepfakes pose serious risks. They can be used to spread misinformation, manipulate public opinion, commit fraud, and misuse a person's identity without consent. These concerns have prompted many countries to introduce regulations, such as restricting the use of deepfakes in elections and requiring AI-generated content to be clearly labeled. This study examines the legal challenges posed by deepfakes and recommends dedicated legislation, stronger liability standards, and effective regulatory frameworks to prevent misuse while encouraging responsible innovation. It emphasizes the need for the law to keep pace with advances in artificial intelligence and safeguard individual rights and public trust. Recognizing both the opportunities and the risks associated with deepfakes, this study proposes a number of policy recommendations aimed at reducing their misuse while preserving their legitimate and creative applications. It argues for the introduction of dedicated legislation, stronger liability standards, and comprehensive regulatory frameworks to address the legal challenges created by deepfake technology. As artificial intelligence continues to evolve, the law must also adapt to ensure that technological innovation is balanced with the protection of individual rights, public trust, and democratic values.

KEYWORDS: Deep fake technology, unfair trade practices, Misleading advertisements, AI generated content, regulatory gap, fake endorsement, market manipulation etc.

INTRODUCTION

Artificial Intelligence (AI) has rapidly transformed the modern business landscape, altering how companies operate, market their products, and engage with their customers. While these technological advancements have improved efficiency and innovation, they have also introduced complex legal and ethical challenges. One of the most concerning trends in this context is the emergence of deepfake technology, which utilizes AI to generate highly realistic yet fabricated audio, video, or visual content. This information can closely resemble real individuals, making it difficult at times to distinguish between authenticity and manipulation. Deepfakes pose significant risks in the commercial sector. They can be used to deceive consumers through fraudulent advertisements, impersonate corporate executives, manipulate the stock market, or damage a competitor's reputation. This not only undermines consumer trust but also disrupts fair competition within the marketplace. The potential for abuse extends beyond isolated incidents, presenting a systemic threat to the integrity of online business practices and corporate accountability. Traditionally, unfair trade practices have been defined as dishonest, fraudulent, or misleading actions by businesses seeking an unfair advantage. However, with the advent of digital technologies, these practices have evolved in both form and complexity. Deepfakes represent a new dimension of deception, as the content produced can be disseminated rapidly and widely, often going unnoticed. Consequently, consumers are increasingly susceptible to misinformation, making it exceedingly difficult to make informed decisions.

LITERATURE REVIEW

The intersection of artificial intelligence and law has garnered increasing attention from scholars. Research indicates that deepfakes pose risks to privacy, democracy, and the integrity of businesses. However, the predominant focus in literature is on criminal law and cybersecurity, rather than business law. Some authors suggest that existing consumer protection laws could be broadened to address deceptive AI practices. Others emphasize the absence of clear statutory provisions, which creates ambiguity in enforcement. While global studies advocate for proactive regulation, research in India tends to focus on a reactive regulatory framework. Consequently, there exists a gap in the examination of deepfake technology, particularly concerning unfair trading practices. Recent studies highlight that deepfake technology represents a significant trend at the intersection of technology and law.

Chesney and Citron (Chesney, Robert & citron, Danielle keats, deep fakes: a looming challenge for privacy, democracy and national security, California law review (2019), assert that deepfakes create a challenge in trusting even authentic evidence, thereby compromising the integrity of both media and the legal system. Other researchers have focused on the potential for deepfake misuse, particularly in areas such as fabricated videos, political manipulation, and non-consensual content. Reports indicate that a significant portion of deepfake material available online has been used maliciously, particularly targeting women. Scholars have also highlighted the role of deepfakes in disseminating misinformation during elections, as they can influence public opinion. Additionally, research exists that examines the repercussions of deepfakes on businesses. Instances of fraud have been reported where criminals utilize AI-generated voices or videos to impersonate company officials, facilitating the transfer of funds or the acquisition of sensitive information. This illustrates that deepfakes pose both social and economic threats to corporations. However, not all studies view deepfakes negatively. Some authors suggest that they have beneficial applications in sectors such as entertainment, education, and healthcare. For example, in the film industry, deepfake technology can significantly reduce production costs, while in the medical field, it can assist individuals who have lost their ability to speak. Overall, the existing literature suggests that deepfakes embody a double-edged technology. While they may foster innovation and provide valuable applications, they also present considerable ethical, legal, and social challenges. Therefore, it is essential to examine both their positive and negative dimensions in a balanced manner.

RESEARCH QUESTION

1. What is a deepfake technology and how it has impacted on business transactions?

2. Does the Indian law consider the use of deepfakes to be an unfair trade practice?

3. Are the existing laws enough to deal with the problem of deepfake misuse?

4. Do they have regulatory loopholes to address business harms associated with deepfakes?

5. What changes need to be done to provide consumer protection and fair competition?

OBJECTIVE

The main aim of this research is to analyze the increasing influence of the deepfake technology on the operations of business, especially regarding unfair trade practices. It aims to know how the artificially-created manipulated content can be abused in business practices to defraud consumers, distort competition, and damage the reputation of businesses. The other important goal is to examine the notion of unfair trade practices in the digital age and to address how the old law relates to technologically advanced varieties of deception like deepfakes. The research will further seek to determine how the current Indian legal system, such as legislations regarding consumer protection, information technology, and intellectual property, is effective in dealing with the issues of deepfake technology. Moreover, the paper aims to pinpoint the gaps and constraints of the existing regulatory framework that can enable the abuse of deepfakes to persist. It also seeks to bring into focus the necessity of having particular legal provisions or policy provisions to address such emerging risks. Lastly, the research aims to propose potential reforms and legal solutions that can contribute to making the business world more transparent, safeguard consumer interests, and ensure healthy competition in the increasingly digital and AI-friendly business environment.

RESEARCH METHODOLOGY

This study uses a doctrinal research approach, which is based on:

- Statutory analysis (Consumer protection act, IT Act)
- Judicial precedents
- Academic literature
- Comparative legal frameworks

It is an analytical and descriptive approach, which aims at determining the gaps in the law and suggests changes. This study is primarily a qualitative study and relies on secondary sources of information. Data has been gathered by utilizing various published sources such as journal articles, research papers, reports and some credible online sources. To this end, databases like 4IEEE Xplore, 5ACM Digital Library, SpringerLink and Scopus were consulted. During the search of the relevant studies, the simple keywords such as deepfake, AI content,misinformation, ethics, and online safety were applied. Peer reviewed articles were considered only to make sure that the information is reliable. The researchers primarily examine the years 2017-2025 since the technology of deepfakes has evolved at an extremely rapid pace over the past years. A large number of articles were identified, but only those were chosen that were directly related to ethical issues, legal, and social impact of deepfakes. Only the technical studies were excluded that did not comment on these aspects. Once the data was collected, it was read and comprehended meticulously, and organized in a simple manner to find out the key problems and effects of deepfake technology.

DEEPFAKES AND MISINFORMATION

Deepfake technology has made it easier than ever to create realistic but false audio and video content. As a result, it has become a powerful tool for spreading misinformation. By manipulating a person's appearance or voice, deepfakes can make it seem as though someone said or did something they never actually did. Since these videos are often difficult to distinguish from genuine content, they can easily mislead the public. This is especially concerning during elections, where deepfakes of political leaders can influence public opinion and undermine trust in democratic processes. Even after such content is exposed as fake, it may continue to create confusion and damage public confidence. The problem is further intensified by social media, where content spreads rapidly with little or no verification. A deepfake video can reach millions of people within a short time, misleading audiences and damaging the reputation of those targeted. Another major concern is that deepfakes undermine trust in authentic information. As people become aware that realistic videos can be fabricated, they may begin to question even genuine evidence, making it increasingly difficult to distinguish truth from falsehood. Overall, deepfake technology has made misinformation more convincing and more harmful, highlighting the need for greater public awareness, stronger legal safeguards, and responsible practices by digital platforms to prevent its misuse.

ABUSE OF DEEPFAKES TO EXPLOIT AND NON-CONSENSUAL CONTENT

The misuse of deepfake technology to create content without a person's consent has become a serious ethical and legal concern. One of the most common forms of abuse involves manipulating images or videos by placing an individual's face onto pornographic or other inappropriate content without their knowledge or permission. Such non-consensual deepfakes violate personal dignity and privacy and can cause lasting harm to a person's reputation, mental well-being, and social relationships. In many cases, victims are unaware of the content until it has already spread widely online. The rapid spread of deepfakes through social media makes the problem even more difficult to address. Once shared, such content is often difficult to remove completely, allowing the harm to persist. The lack of public awareness and the tendency to share content without verifying its authenticity further contribute to the problem. As a result, deepfake technology, instead of serving as a tool for innovation, can become a means of exploitation. This highlights the urgent need for stronger legal protections, greater public awareness, and increased accountability to prevent the creation and spread of non-consensual deepfake content.

DEEPFAKES AND CYBERSECURITY THREATS

Deepfake technology has evolved far beyond its initial use in entertainment and digital media. Today, it poses significant cybersecurity challenges by enabling highly convincing forms of deception that exploit trust, identity, and human judgment. Unlike traditional cyberattacks that rely primarily on technical vulnerabilities, deepfakes manipulate human perception, making them one of the most difficult emerging threats to detect and prevent. As artificial intelligence continues to improve, the ability to create realistic fake audio, video, and images has become more accessible, increasing the risk of misuse by cybercriminals, fraudsters, and malicious actors.

One of the most serious cybersecurity risks associated with deepfakes is identity impersonation. By cloning a person's face or voice, attackers can convincingly impersonate corporate executives, government officials, financial institutions, or even family members. Such impersonation can be used to deceive employees into transferring funds, disclosing confidential information, or granting unauthorized access to secure systems. Several real-world incidents have demonstrated how AI-generated voice cloning has been used to trick employees into believing they were receiving instructions from senior executives, resulting in substantial financial losses. These attacks exploit human trust rather than technical weaknesses, making them particularly difficult to prevent through conventional cybersecurity measures. Deepfakes have also significantly increased the effectiveness of social engineering attacks. Traditionally, cybercriminals relied on phishing emails or text messages to manipulate victims. However, artificial intelligence now enables attackers to create realistic video calls, voice messages, and live interactions that appear completely genuine. A familiar face or recognizable voice often creates a false sense of authenticity, making victims

more likely to comply with fraudulent requests. This evolution has made phishing attacks more sophisticated and greatly reduced the effectiveness of traditional awareness measures that focus only on suspicious emails or links. Another major concern is the spread of misinformation and reputational attacks. Deepfake videos can falsely portray business leaders, politicians, celebrities, or public officials making controversial statements or engaging in conduct that never occurred. Such fabricated content can spread rapidly through social media, influencing public opinion before its authenticity can be verified. For businesses, these attacks may damage brand reputation, reduce consumer confidence, affect investor decisions, and even influence stock prices. Governments may also face threats to national security if deepfakes are used to create false emergency announcements or manipulate public perception during elections, conflicts, or public crises. Deepfakes also pose a growing threat to biometric authentication systems. Many organizations increasingly rely on facial recognition, voice recognition, or other biometric technologies to verify identity and control access to secure facilities or digital platforms. If these systems lack effective anti-spoofing capabilities, sophisticated deepfakes may bypass authentication mechanisms by presenting highly realistic synthetic faces or cloned voices. Unauthorized access to sensitive databases, financial systems, healthcare records, or government infrastructure could have severe legal, economic, and security consequences.

The increasing availability of artificial intelligence tools has further intensified these risks. Earlier, producing convincing fake videos required specialized technical expertise and expensive software. Today, AI-powered applications and publicly available platforms allow individuals with little technical knowledge to create highly realistic deepfake content within minutes. This widespread accessibility has lowered the barrier to cybercrime, making deepfake-enabled fraud more frequent and more difficult for organizations to anticipate. Addressing these cybersecurity challenges requires a combination of technological, organizational, and legal responses. Organizations should adopt multi-factor authentication rather than relying solely on voice or facial recognition for identity verification. Sensitive financial transactions and requests involving confidential information should require independent verification through multiple communication channels. Regular cybersecurity training should educate employees about deepfake-enabled fraud, voice cloning, and AI-assisted phishing techniques so they can recognize suspicious requests even when they appear authentic. Companies should invest in AI-based deepfake detection technologies capable of identifying manipulated audio and video before they are used for authentication or communication. Security systems should incorporate liveness detection, behavioural analysis, and continuous monitoring to reduce the risk of biometric spoofing. Governments and regulatory authorities also have an important role in establishing standards for AI-generated content, promoting responsible AI development, and encouraging collaboration between technology companies, cybersecurity experts, and law enforcement agencies.

Public awareness is equally important. Individuals should exercise caution before trusting audio or video messages that request urgent financial transfers, confidential information, or access credentials, even when they appear to come from trusted sources. Verifying requests through an independent communication channel can significantly reduce the likelihood of becoming a victim of deepfake-enabled fraud. Deepfakes have fundamentally changed the nature of cybersecurity threats by combining artificial intelligence with psychological manipulation. They blur the distinction between authentic and fabricated content, making deception more convincing than ever before. As deepfake technology continues to advance, effective cybersecurity will depend not only on stronger technical safeguards but also on legal regulation, organizational preparedness, and increased public awareness. A comprehensive approach that integrates technology, law, education, and responsible AI governance is essential to minimize the risks posed by deepfakes while allowing society to benefit from the legitimate applications of artificial intelligence.

DEEPFAKE TECHNOLOGY CONCEPT

Deepfakes are AI-generated media created using deep learning and neural networks to produce highly realistic images, videos, and audio that closely imitate real people. While they have legitimate uses in areas such as film production, virtual marketing, and digital content creation, they are also widely misused for fake celebrity endorsements, fraudulent advertisements, corporate misinformation, and identity fraud.

The growing sophistication of deepfakes poses significant risks across multiple sectors. In politics, they can spread misinformation and influence public opinion; in healthcare, they may contribute to false medical information; in entertainment, they can damage reputations; and in banking, they enable financial fraud through forged documents, voice cloning, and impersonation during video calls. Deepfakes also pose serious cybersecurity challenges by facilitating synthetic identity fraud and making it increasingly difficult to distinguish authentic content from manipulated media. Although existing research has largely focused on the technological and legal aspects of deepfakes, less attention has been given to their impact on organizations. Managers may unknowingly rely on manipulated content, leading to poor strategic decisions, financial losses, and reputational harm. The widespread availability of deepfake creation tools has further increased these risks by making manipulated content easier to produce and harder to trace. Therefore, organizations must adopt advanced AI-based detection systems, visual recognition technologies, and strong verification mechanisms to safeguard decision-making processes. Further research is needed to understand how businesses can effectively manage the risks of deepfakes while benefiting from their legitimate applications.

DEEPFAKE UNFAIR TRADES

In Section 2(47) of the Consumer Protection Act, 2019, misleading advertisements and false representations are considered as unfair trade practices. Deepfakes can:

- Fraudulent endorsement by celebrities.
- Fraud against consumers on quality of products.
- Manipulate purchasing decisions

Example: A case of a deep fake video of a well-known person advertising some product against his or her will can alter the way people behave, which is considered to be a form of deception. Recent studies have shown that deepfakes are a major threat to financial markets because they can be used to manipulate stocks or impersonate and mislead investors, and hyper realistic fake news can be strongly responded to by investors. The major works point to the necessity of sophisticated detection because deepfakes are able to evade the existing 6Section 2(47), consumer protection act, 2019.

INDIAN LEGAL SYSTEM

India presently lacks a dedicated statute to regulate deepfake technology. While certain provisions in existing laws can be invoked, they were not designed for AI-generated synthetic media and therefore suffer from conceptual and enforcement limitations. The key gaps are as follows:

1. Consumer Protection Act, 2019

Scope: The Act defines “misleading advertisement” under Section 2(28) and provides for penalties against false or deceptive claims under Section 89. The Central Consumer Protection Authority can order discontinuation of such ads.

Gap: The Act does not recognize “AI-generated deception” as a distinct category. Deepfakes used for fake product endorsements, cloned voice scams in customer service, or synthetic influencer marketing fall outside its express language. Enforcement depends on interpreting “misleading” broadly, which creates uncertainty. There is no mandate for platforms to disclose whether an endorsement is synthetic, and no specific liability for generative AI tools that enable mass production of fake reviews or ads. The Act also provides no remedy for non-commercial harms like reputational damage from personal deepfakes.

2. Information Technology Act, 2000

Scope: Section 66D penalizes cheating by personation using a computer resource. Section 66E covers violation of privacy by capturing or publishing images of private areas. Section 67 and 67A deal with obscene and sexually explicit content. Section 69A allows blocking of content threatening sovereignty or public order.

Gap: Section 66D requires "personation" and "cheating," which are difficult to establish when a deepfake does not directly solicit money or when the victim is the person depicted rather than the viewer. The law does not cover non-consensual synthetic sexual content that is not "captured" but entirely AI-generated, so Section 66E may not apply. Takedown under Section 69A is discretionary and episodic, not a systemic solution. The IT Rules 2021 impose due diligence on intermediaries, but they do not define "synthetic media" or mandate AI-detection and labeling. Consequently, platforms claim safe harbor under Section 79 even when hosting viral deepfakes, and enforcement remains reactive.

3. Indian Penal Code / Bharatiya Nyaya Sanhita, 2023

Scope: BNS provisions on cheating under Section 318, forgery under Section 336, defamation under Section 356, and outraging modesty under Section 73 can be invoked. Police often file cases under these sections for deepfake incidents.

Gap: These provisions lack technical specificity. "Cheating" requires dishonest inducement of property delivery, which does not cover reputational or electoral harm. "Forgery" traditionally applies to documents, and courts are yet to settle whether synthetic video is a "document" under Section 2(7) of BSA. Defamation requires proof of malice and offers truth as a defense, which is ill-fitted for content that is entirely fabricated but believable. The law does not address the unique mens rea issues in AI, such as when a user prompts a tool without intent to harm but the output is misused by others. Sentencing is not graded by scale of harm, so a deepfake seen by 10 million people attracts the same penalty as a single defamatory statement.

4. Competition Act, 2002

Scope: The Act prohibits anti-competitive agreements under Section 3 and abuse of dominance under Section 4. The Competition Commission of India can penalize unfair trade practices that distort the market.

Gap: Deepfakes can manipulate competition through fake CEO statements that crash stock prices, synthetic product failure videos that harm rivals, or false celebrity endorsements that divert consumers. However, the Act has no jurisprudence on "information manipulation" as an anti-competitive practice. Establishing "agreement" or "dominance" is difficult when the actor is an anonymous user or foreign platform. There is no fast-track mechanism to address viral disinformation that causes immediate market harm. The enforcement timeline of CCI investigations is incompatible with the speed at which deepfakes spread. Further, the Act does not empower CCI to demand algorithmic audits of generative AI tools that may be used for market manipulation.

Overall Assessment

The existing laws are anthropocentric, document-centric, and transaction-centric. Deepfakes challenge all three assumptions because they create new realities rather than misrepresent existing ones, exist as code rather than paper, and cause dignitary, electoral, and systemic harms beyond individual financial loss. Reliance on general provisions leads to inconsistent FIRs, low conviction rates, and forum shopping by victims. Without definitional clarity, graded liability, mandatory disclosure standards, and platform accountability, India's legal system will remain reactive and inadequate to address the scale, speed, and sophistication of AI-generated deception

LEGAL PROTECTION OF PERSONALITY RIGHTS AND RELATIVES LAWS

Due to the emergence of deepfake technology, the security of identity and personal image has never been as significant as it is now. This has a direct impact on the personality rights of an individual when his or her face, voice or likeness is employed without consent. The rights are associated with the identity of a person, his dignity, and privacy, although they are not always clearly outlined in a single law. In most instances, the various fields of law are applied in combination when addressing such issues. The intellectual property acts, particularly the image rights and passing off may sometimes be involved in case the identity of an individual is abused in order to carry out business activities. In case, faking advertisement using the face of a person, without their permission, may result in a lawsuit. Beyond this, there are also privacy laws that are also important. Their privacy may be regarded as infringed upon by the use of a person image or voice without their consent. There has been an observation by courts that people have a right to how their personal identity is used, particularly in the digital space. Additional legal regulations, such as cyber laws, might also be applicable in case deepfakes are used to commit harm e.g. harassment, defamation, or fraud. Nonetheless, among the primary issues is the fact that the current legislation was not explicitly created to address more sophisticated technologies such as deepfakes. Due to this fact, there are still loopholes in the effectiveness with which such cases could be addressed. In general, although various legal regimes provide certain protection, there is an increasing need to provide clearer and more specific regulations to deal with the abuse of deepfake technology and to further protect the right to personality.

IP PROTECTION LEGAL INSTRUMENTS

The court allowed infringement of a registered mark of a well-known personality an injunction under trademark and passing off. This was due to the fact that the plaintiff had a caricature that was covered in the Preview of the goods being sold, which leads to infringement of the registered mark. Exploitation of a well-the distinguishing feature of known personality, too, is an unfair competition, deserving of a passing-off claim. Their uniqueness is also used in an illegitimate manner which gives a false appearance of a deception plaintiff has licensed or otherwise has a relationship with the goods or services of the defendant, which is similar to fraudulent endorsement. The court can in extraordinary situations apply copyright to guard personality rights although the Act is not clearly stated to the same. Some of the 11provisions of the Copyright Act could be helpful remedies against violation of personal rights. Section 2(qq), for example, defines performer if The performer definition falls under personality; Section 38 which stated performer right, forbids the unauthorized promotion of one's performance. Section 57 also provides ethical safeguards in certain cases and forbids the illegal advertisement of performance. Ethical is also provided in section 57 protections in specific instances.

DEEPFAKE-TECHNOLOGY COPYRIGHT

Deepfakes technology has raised several questions about the problem of copyright and ownership of content. Since deep fakes are generally created using the existing images or videos and sound clips, one would need to understand whether it is allowed to use them or not. In the majority of cases, the material initially belonged to another person and stealing the material without their permission can lead to copyright problems. Supposing that a video clip of a film or a speech of some influential person is stolen and then processed with the assistance of deepfake, it could still be considered the property of the initial author. Even in cases of such content being modified or edited, it does not always result in being completely new and not liable to copyright claims. Because of this fact, the inventors of deepfakes might at times be culpable of using a guarded material without the necessary rights. The other issue is the copyright of the final product of the deepfake. Not necessarily, it is the person who has created the deepfake, the person who has been used in the deepfake or the person who created the original material who is the real owner. This leads to confusion especially where this is used in a business manner. The other example is when deepfakes are misapplied via fake endorsement or advertisements. It is not only a copyright issue, but, a case of unfair use of identity of a person, in this instance. Overall, the existing copyright regulations provide some safeguarding, but, they are not ready enough to tackle the problem of deepfakes technology. It causes the necessity to rethink the means by which the copyright regulations may be applied to AI-generated material.

INFORMATION TECHNOLOGY ACT PROVISIONS

In India, no legislation is directly concerned with deepfake technology, but there are also certain provisions of the Information Technology Act, which may be relevant in particular, based on the application of the technology. These laws primarily revolve around matters such as security on the internet, abuse of digital information, identity theft and privacy invasion. In cases where deepfakes are deployed to produce or disseminate malicious or deceptive information, and particularly that which impacts the reputation or dignity of a person, legal repercussions might arise. To illustrate, when a person makes a video or photo look like they put the person in a situation that is not real or offensive and shares it on the Internet, it can be considered as harmful digital content. In this situation the victim has a right to sue. There are certain issues that I have observed. Deepfake technology is able to replicate the face or voice of a person and impersonate him or her. In case it is done to defraud another person or to get money, it can fall within the category of impersonation offences and Internet-related fraud. Such abuse has become more widespread with the evolution of AI tools, as it is easier to fool individuals. Privacy is another issue of concern. When a personal picture, video or voice recording of a person are utilized without their consent to generate deepfake content, this can be considered as an intrusion on their privacy. This is all the more grave when the content is private or sensitive in nature and is posted publicly without permission. Online platforms are also significant besides individuals. The social media companies along with other intermediaries should be responsible and sensitive to eliminate the harmful or illegal content when they are informed of such actions. Nevertheless, in reality, it is hard to control the proliferation of deepfake material due to the fact that within minutes such content can become viral and reach many individuals before anything can be done. A second challenge is that a good portion of the users are not well informed of deepfake technology. Due to this, they can find and post such content without verifying whether it is authentic or not. This is terribly detrimental to new generation. In general, although the Information Technology Act does offer certain degree of protection in instances of misuse of deepfakes, it was not created with the purpose of dealing with such a sophisticated technology. Due to this, gaps exist in the existing legal system. This indicates that there is a need to have more clear rules, greater awareness, and, enforcement of the same in order to contend with the increasing dangers of deepfakes.

COMPRATIVE INTERNATIONAL PRESPECTIVE

This problem of deepfakes has already started to be treated in various countries differently, however, on the global level, the strategy has not been developed yet. Other countries have gone ahead to take the initiative too early to guard against the misuse of this technology especially when it is about privacy, elections or even the safety of masses. The strategy is not established in the United States yet. Instead of one law, different states have developed their own laws. To illustrate, the use of deepfake videos during elections has been criminalised in some states as a way of deceiving voters. There are also laws to non-consent explicit material that has been created using deepfakes. In the meantime, the issue of security of freedom of speech receives a lot of attention, thus complicating regulation sometimes. In the European Union, priority is given to safety of the users and protection of data. Legislation on data privacy and legislation on digital services are likely to be used to deal with the challenges of deepfakes. EU has been working diligently to come up with more inclusive AI laws that will hold technology companies more responsible in the application of their applications. The EU strategy is more preventative and organized relative to other areas. China has become more hard line on deepfakes. It has also instituted rules that entail labeling of the AI-generated content in a transparent way such that the users are capable of differentiating between the real and the not. The platforms will also be more aggressive in checking and deleting harmful content. This is a less assertive approach whereby the government emerges as a force to reckon with. In these nations as the United Kingdom, the issue is debatable and the existing laws regarding the harm and abuse of digital materials on the Internet are applied where possible. It is beginning to be accepted that it may be necessary that some rules are in place in future as the technology continues to expand. In comparison to these countries, India is still at its early stages of deepfakes. Even though some laws might be applicable, no particular or direct framework exists yet. When we consider how other countries are doing things, one can observe that there has to be a middle ground that will not only make the people safe, but be able to facilitate innovation at the same time. Overall, the state of affairs in the world suggests that the issue of deepfakes technology is a widespread phenomenon, but, countries are

solving it differently, basing on their legal frameworks and priorities. This is the reason why it is important to have various countries learn and develop more effective ways of dealing with the risks.

REGULAR LOOPHOLES AND BARRIERS

1. There is no legal definition of deepfakes.

2. Problems of detection and enforcement

3. No liability of creators and platforms.

4. Issues of jurisdiction of digital content.

5. Lack of awareness of consumers.

SIGNIFICANT UNFAIR TRADE PRACTICE LOOPHOLES

Impersonation Fraud (Vishing/Phishing): Fraudsters use the AI-generated voice or video of executives to approve an urgent transfer of wire or disclose sensitive data. Reputational Warfare: The use of fake videos of competitors or employees is targeted at manipulating the price of stock or damaging the brand reputation. Dark Patterns and Deception: Unethical marketing techniques like using deepfakes to entice consumers into buying products or relying on websites.

Evidentiary Gaps: AI is a black box, thus difficult to establish liability, in a corporate conflict or establish authenticity Data Scraping Exemptions: At times, the laws fail to safeguard privacy of publicly-available data, and this presents a chance to the attackers to train AI models on social media data without consent.

RECOMMENDATIONS

A. To effectively regulate deepfake technology in India, it is suggested that a dedicated law be enacted to clearly define deepfakes and create a graded liability framework that distinguishes between permissible uses like art and satire, civil violations for unlabeled content, and criminal offences for non-consensual sexual deepfakes, election-related deepfakes, and content inciting violence.

B. The law should mandate prior consent for creating deepfakes of identifiable individuals and require both visible and invisible disclosure of all AI-generated content, with social media platforms made responsible for detecting and auto-labeling synthetic media.

C. Safe harbor protection under the IT Act should be limited for websites that primarily host malicious deepfakes, and MeitY should be empowered to block such sites while payment gateways deny them services. For consumer protection, a single-window portal like StopDeepfake.gov.in should be launched for fast reporting, takedown, and legal aid, alongside amendments to the DPDP Act to strengthen the right to be forgotten against synthetic impersonation and the creation of a victim compensation fund.

D. Public awareness should be enhanced through synthetic media literacy in curricula and free detection tools, while AI developers must be held accountable through mandatory red-teaming and compliance reports. Together, these measures would ensure a balanced approach that curbs misuse without hindering innovation.

CONCLUSION

According to the general discussion, it is clear that the deepfake technology is growing swiftly and that it is penetrating the everyday digital world. Despite the fact that it started out as a creativity and entertainment tool, it has been misused in most of its applications especially in the spread of misinformation, harm to personal reputation and production of non-consent content. This makes it a burdensome matter to people and the whole society. One of the biggest problems with deepfakes is the fact that it is difficult to believe what we read and hear on the Internet. It is simple to become a victim of counterfeit content when it seems to be genuine. In the meantime, even the genuine material can be doubted, and this misunderstanding and mistrust of media, institutions, even the legal systems are undermined. It shows that the effect of deepfakes is not limited to technology and the principle of the truth

in the realm of the Internet. The paper also discloses that although there are some legal provisions, they are not fully prepared to handle the issues that deepfakes have caused. In other countries like India, a situation can exist where the existing laws can be applied, but there is no definite and specific rules. Comparing it with other countries, it is possible to note that it should be more specifically targeted, in particular, regulation, awareness, and platform responsibility. In the meantime, it is important to understand that deepfake technology is not bad per se. It can as well be applied in other sectors like education, entertainment and healthcare. Because of this, the idea that it should be the objective to completely restrict the technology, however, to ensure that it is used in a responsible way.

REFRENCES

1. Consumer Protection Act, No. 35 of 2019 (India).
2. Information Technology Act, No. 21 of 2000 (India).
3. Indian Penal Code, No. 45 of 1860 (India).
4. K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 (India).
5. John Doe, Artificial Intelligence and Consumer Protection, 45 Indian L. Rev.121 (2020).
6. European Commission, Proposal for Artificial Intelligence Act (2021).
7. Robert Chesney & Danielle Citron, Deepfakes and the Law, 107 Calif. L. Rev.1753 (2019).
8. Indian evidence Act,1872- relevance of electronic device
9. Anvar P.V. v. P.K. Basheer, (2014) – admissibility of electronic evidence.
10. Justice K.S. Puttaswamy (Retd.) v. Union of India (Aadhaar case), (2018) data protection concerns.
11. Sabu Mathew George v. Union of India, (2017) – responsibility of online platforms.
12. Google India Pvt. Ltd. v. Visaka Industries, (2020) – intermediary liability.
13. Swami Ramdev v. Facebook Inc., (2019) – removal of harmful online content globally.

Research Papers and Journal Articles

1. Deepfake Detection and Its Challenges, ACM Computing Surveys.
2. Synthetic Media and the Future of Trust, MIT Technology Review.
3. AI and Corporate Fraud Risks,Journal of Financial Crime.
4. Regulating Artificial Intelligence in Business Journal of Business Law.
5. Consumer Protection in the Age of AI, National Law School Journal.
6. Impact of Deepfakes on Brand Reputation, Journal of Marketing Analytics.
7. Cybersecurity Threats from AI-generated Content, Journal of Cybersecurity.

International Reports and Guidelines

1. OECD Principles on Artificial Intelligence (2019).
2. UNESCO Recommendation on Ethics of Artificial Intelligence (2021).
3. World Bank Report on Digital Economy and AI Risks.
4. Europol Report: Facing Reality? Law Enforcement and Deepfakes (2022).
5. United Nations Report on Cybercrime and Emerging Technologies