CONSTITUTIONAL CHALLENGES IN DEEP FAKE TECHNOLOGY: RETHINKING CRIMINAL LIABILITY IN THE DIGITAL ERA

Tharunika JD, BCA LLB (Hons), School of Excellence in Law, Tamil Nadu Dr. Ambedkar Law University, Chennai – 113, India

Boopathi A, B.Com LLB (Hons), School of Excellence in Law, Tamil Nadu Dr. Ambedkar Law University, Chennai – 113, India

ABSTRACT

Deep fake technology, driven by advancements in artificial intelligence and machine learning, has emerged as one of the most significant challenges confronting constitutional governance and criminal justice systems in the digital era. While synthetic media offers legitimate benefits in areas such as education, healthcare, entertainment, and digital communication, its misuse has created serious threats to privacy, dignity, reputation, democratic integrity, and public trust. This study critically examines the constitutional and criminal law implications of deep fake technology, with particular emphasis on the tension between freedom of speech and the protection of fundamental rights. Adopting a combined doctrinal and empirical methodology, the research analyses constitutional provisions, statutory frameworks, judicial precedents, and primary data collected from 125 law students and legal professionals. The findings reveal that existing legal mechanisms are insufficient to address the complex challenges posed by AI-generated content, particularly in relation to mens rea, attribution of liability, intermediary responsibility, and evidentiary authenticity. The study contends that deep fake challenge the foundational assumptions of traditional criminal jurisprudence by disrupting established concepts of intent, causation, authorship, and evidentiary reliability. It further argues that conventional models of criminal liability are increasingly ineffective within a digital ecosystem characterised by anonymity, automation, and rapid dissemination of information. The research advocates a balanced, rights-based, and future-oriented regulatory framework that ensures accountability, safeguards constitutional freedoms, protects victims, and promotes responsible technological innovation. Ultimately, the study demonstrates that effective governance of deep fake technology requires a fundamental rethinking of constitutional protections and criminal responsibility to preserve truth, justice, and democratic trust in the age of artificial intelligence.

Keywords: Deepfake Technology, Constitutional Rights, Criminal Liability, Artificial Intelligence and Digital Governance.

INTRODUCTION:

The rapid evolution of artificial intelligence has given rise to deep fake technology, a sophisticated form of synthetic media capable of creating highly realistic but fabricated audio, video, and image content. Although deep fake technology has beneficial applications in entertainment, education, healthcare, and digital innovation, its misuse has generated serious constitutional, legal, and ethical concerns across the globe. Deep fake technology poses an unprecedented threat to democratic institutions and individual rights, sparking a fierce constitutional debate. Criminal justice systems globally are struggling to balance the protection of personal dignity, privacy, and reputation against the fundamental guarantee of freedom of speech and expression, thereby creating a dangerous legal grey area where malicious actors can easily evade liability.

The growing misuse of deep fake in political propaganda, electoral manipulation, misinformation campaigns, cyber fraud, identity theft, revenge pornography, and defamation has exposed the limitations of existing legal and regulatory mechanisms. Unlike traditional forms of digital manipulation, deep fake possess the power to distort public perception, undermine trust in democratic processes, and blur the distinction between truth and fabricated reality. In a digital society where information spreads instantly, even a single manipulated video or audio clip can trigger social unrest, influence elections, damage reputations, and violate fundamental human rights within moments. This emerging technological threat challenges core constitutional principles relating to privacy, dignity, equality, free speech, due process, and accountability. Existing criminal laws were primarily designed to address conventional offences and are often inadequate to determine liability in cases involving AI-generated synthetic media.

In India, the absence of a specific statutory framework governing Deep fake further complicates constitutional enforcement and criminal accountability in the digital sphere. Questions regarding who should bear criminal responsibility - the creator, developer, distributor, platform provider, or user remain largely unresolved. Furthermore, Deep fake complicate traditional legal doctrines such as mens rea, evidentiary authenticity, jurisdiction in cyberspace, and the constitutional limits of state regulation over digital expression.

Against this backdrop, the topic “Constitutional Challenges in Deep fake Technology: Rethinking Criminal Liability in the Digital Era” critically examines the constitutional tensions

created by Deep fake technology and evaluates whether existing legal systems are capable of addressing its evolving dangers. The study argues that traditional models of criminal liability are insufficient to address the decentralized, anonymous, and technologically complex nature of deep fake -related harms. The study seeks to explore the need for a balanced constitutional and criminal law framework that protects democratic integrity and individual rights while preserving legitimate technological innovation and freedom of expression in the digital era.

REVIEW OF LITERATURE:

Citron and Chesney, The review of existing literature reveals that Deep fake technology has emerged as one of the most controversial developments in artificial intelligence and digital communication. Contemporary academic discourse increasingly examines deep fake not merely as technological tools but as constitutional, legal, ethical, and democratic challenges capable of disrupting social trust, informational authenticity, and individual rights. Scholars such as Danielle Citron and Robert Chesney argue that traditional legal systems are inadequate to regulate AI-generated synthetic media while simultaneously preserving constitutional freedoms such as freedom of speech and expression. Existing scholarship therefore emphasizes the urgent necessity for constitutional and criminal law reforms capable of balancing technological innovation with human rights protections.

Lan Goodfellow, Early academic studies on Deep fake technology primarily focused on advancements in artificial intelligence, machine learning, and neural network systems used to generate synthetic audio-visual content. Technological researchers initially highlighted the beneficial applications of deep fake in entertainment, cinema, healthcare, education, accessibility technologies, virtual communication, and digital innovation. Scholars such as Lan Goodfellow emphasized the transformative potential of generative AI systems capable of reshaping digital creativity and communication. However, with the rapid expansion of social media platforms and generative AI tools, academic attention gradually shifted toward concerns relating to cybercrime, misinformation, impersonation, identity theft, revenge pornography, reputational exploitation, and constitutional harm.

Hany Farid, A substantial body of contemporary literature identifies deep fake as a direct threat to democratic institutions and constitutional governance. Scholars including Hany Farid argue that deep fake -enabled misinformation possesses the ability to manipulate electoral behaviour, influence public opinion, weaken democratic accountability, and erode public confidence in

media authenticity. Existing studies further observe that deep fake blur the distinction between truth and fabrication, thereby generating widespread informational distrust within democratic societies. Academic commentators emphasize that in constitutional democracies dependent upon informed public participation, synthetic media threatens not only individual rights but also the structural legitimacy of democratic institutions themselves.

Anita Allen, Academic literature concerning privacy and human dignity further contends that deep fake misuse constitutes a severe violation of personal autonomy and identity rights. Scholars including Anita Allen emphasize the alarming rise of non-consensual deep fake pornography, impersonation, identity manipulation, and reputational exploitation, particularly targeting women and public figures. Existing literature frequently associates these harms with constitutional protections relating to informational privacy, psychological integrity, dignity, and the right to reputation. Researchers argue that victims of deep fake abuse often suffer long-term emotional, social, economic, and professional consequences that existing legal remedies inadequately address. This demonstrates that the impact of deep fake technology extends beyond cybercrime into broader constitutional and human rights concerns.

Jack Balkin, The literature also identifies substantial shortcomings within traditional criminal law frameworks when applied to Deep fake -related offences. Contemporary legal scholarship observes that conventional criminal doctrines such as mens rea, causation, intention, attribution, evidentiary authenticity, and jurisdiction become increasingly difficult to establish within decentralized digital ecosystems driven by artificial intelligence technologies. Scholars such as Jack Balkin argue that digital platforms and algorithmic systems challenge traditional theories of accountability and legal responsibility. Existing academic debate further questions whether criminal liability should extend solely to creators of malicious deep fake or also encompass software developers, intermediaries, online platforms, and users who knowingly circulate manipulated content. Such scholarly uncertainty reflects a broader recognition that traditional models of criminal responsibility may no longer adequately respond to technologically sophisticated forms of cyber harm.

In the K.S. Puttaswamy judgment, the Supreme Court of India recognized privacy as a fundamental right under Articles 14, 19, and 21 of the Constitution. The Court emphasized that privacy includes protection of personal autonomy, dignity, identity, and informational control. Although the judgment was delivered before the emergence of Deep fake technology as a

major concern, its recognition of informational privacy provides a constitutional foundation for addressing unauthorized digital manipulation of an individual's image, voice, and personal data. The decision underscores that technological advancements must operate within constitutional limits and respect individual privacy rights.

RESEARCH GAP:

Existing literature on deep fake technology mainly focuses on technology, cyber security, privacy, and misinformation issues. However, limited studies examine deep fake from a combined constitutional and criminal law perspective. Few studies analyse the application of mens rea, attribution, intermediary liability, and evidentiary challenges to AI-generated content. In the Indian context, research is largely confined to general discussions under the Information Technology Act, 2000. This study bridges the gap by combining constitutional analysis, criminal liability concerns, and empirical findings to suggest a balanced legal framework for regulating deep fake harms in the digital era.

STATEMENT OF THE PROBLEM:

The rapid growth of deep fake technology has created serious constitutional and criminal law challenges by enabling sophisticated forms of misinformation, identity manipulation, and digital deception capable of undermining democratic integrity and individual rights. Existing legal frameworks remain inadequate to address issues relating to criminal liability, evidentiary authenticity, intermediary accountability, and constitutional protection in the digital era. In India, the absence of a dedicated statutory framework regulating deep fake has created significant uncertainty regarding privacy, dignity, free speech, and cyber accountability. Consequently, the increasing misuse of AI-generated synthetic media necessitates a critical rethinking of constitutional governance and traditional models of criminal liability in response to emerging technological realities.

OBJECTIVES OF THE STUDY:

1. To examine the constitutional challenges created by deep fake technology relating to privacy, dignity, democracy, and freedom of speech in the digital era.

2. To analyse the gaps in existing criminal laws and study the application of mens rea, attribution, evidentiary authenticity, and intermediary liability in relation to deep fake.

3. To evaluate the effectiveness of current laws, especially the Information Technology Act, 2000, and suggest a suitable legal framework to regulate deep fake harms while balancing constitutional rights and technological growth.

RESEARCH METHODOLOGY:

This study adopts both doctrinal and empirical research methods to examine the constitutional challenges arising from deep fake technology and the need to rethink criminal liability in the digital era. Under the doctrinal method, the study analyses primary legal sources such as the Constitution of India, Bharatiya Nyaya Sanhita, 2023, Information Technology Act, 2000, relevant judicial decisions, government reports, and other legal materials to understand the present legal framework relating to Deep fake technology, constitutional rights, and criminal liability. The study also makes use of secondary sources including books, law journals, research articles, legal commentaries, newspapers, online legal databases, and reliable websites to examine academic opinions, legal developments, and contemporary issues connected with the topic. Further, an empirical method is adopted through a questionnaire survey conducted among 125 respondents consisting of law students and lawyers to collect their opinions, awareness, and views regarding deep fake technology, constitutional concerns, and the adequacy of existing criminal laws. The collected data is analysed through a qualitative and analytical approach to identify legal challenges, constitutional issues, and possible reforms relating to criminal liability in the digital era.

RESULTS AND DISCUSSION:

Table 1. Demographic Profile of the Respondents

S. No	Particulars	Option	Respondents	Percentage
1	Gender	Male	68	54
		Female	54	43
		Others	0	0
2	Occupation	Law Students	80	64
		Lawyers	45	36
		Others	0	0
3	Age	18–24 years	71	57
		25–40 years	39	31
		Above 40 years	15	12

4	Marital Status	Unmarried	86	69
		Married	39	31

Sources – primary data

Interpretation:

The data in Table 1 is collected from the primary questionnaire conducted among 125 respondents. In terms of gender, the respondents include 68 males (54%), 54 females (43%), and no respondents under the others category. Based on occupation, 80 respondents (64%) are law students and 45 respondents (36%) are lawyers, while there are no respondents from other occupations. Regarding age, 71 respondents (57%) belong to the 18–24 years category, 39 respondents (31%) belong to the 25–40 years category, and 15 respondents (12%) are above 40 years of age. With respect to marital status, 86 respondents (69%) are unmarried and 39 respondents (31%) are married. The participation of respondents from different gender, age, and professional backgrounds provides varied opinions on deep fake technology, constitutional challenges, and criminal liability, thereby increasing the relevance and reliability of the study.

Table 2. Awareness and Constitutional Concerns relating to deep fake Technology

S.No	Particulars	Options	Respondents	Percentage
1	Are you aware of Deep fake technology?	Yes	104	83
		No	21	17
2	Do deep fake affect privacy and dignity rights?	Yes	97	78
		No	28	22
3	Can deep fake threaten democratic integrity and free speech?	Yes	92	74
		No	33	26

Sources – Primary Data

Interpretation:

The data in Table 2 is obtained from the questionnaire responses of 125 law students and lawyers. Among them, 104 respondents (83%) are aware of deep fake technology, while 21

respondents (17%) are not aware. Further, 97 respondents (78%) believe that deep fake affect constitutional rights such as privacy and dignity, and 92 respondents (74%) agree that deep fake can threaten democratic integrity and freedom of speech. The findings indicate a strong understanding among respondents regarding the constitutional implications of AI-generated synthetic media.

Table 3. Criminal Liability and Adequacy of Existing Laws

S.No	Statement	Agree	Neutral	Disagree
1	Existing criminal laws are sufficient to regulate Deep fake harms	31 (25)	20 (16)	74 (59)
2	Current laws face difficulties in applying criminal liability to AI-generated content	81 (65)	22 (18)	22 (17)
3	Mens rea and attribution create challenges in Deep fake cases	88 (70)	19 (15)	18 (15)
4	Digital platforms should bear legal responsibility for harmful deep fake	91 (73)	17 (14)	17 (13)

Sources – Primary Data

Interpretation:

Table 3 reflects respondents' views regarding criminal liability and legal regulation of deep fake. A majority of respondents, 74 (59%), disagree that existing criminal laws are fully sufficient to regulate Deep fake harms. 81 respondents (65%) agree that current legal systems face difficulties in applying criminal liability to AI-generated content. Further, 88 respondents (70%) agree that issues such as mens rea and attribution create legal challenges in Deep fake - related offences. Importantly, 91 respondents (73%) support legal responsibility for digital platforms dealing with harmful deep fake content. These responses show concerns regarding the adequacy of present criminal law mechanisms.

Table 4. Effectiveness of Existing Legal Framework and Need for Reform

S.No	Statement	Agree	Neutral	Disagree
1	The Information Technology Act, 2000 is effective in regulating deep fake	34 (27)	28 (23)	63 (50)
2	India requires a separate legal framework for Deep fake regulation	96 (77)	14 (11)	15 (12)
3	Legal regulation should balance constitutional rights and technological innovation	102 (82)	12 (10)	11 (8)

Sources – Primary Data

Interpretation:

Table 4 presents opinions regarding the effectiveness of the present legal framework and the need for reform. 63 respondents (50%) disagree that the Information Technology Act, 2000 is fully effective in regulating deep fake technology. A significant majority, 96 respondents (77%), support the need for a separate legal framework for deep fake regulation. Further, 102 respondents (82%) agree that any future legal framework should balance constitutional rights with technological innovation. These findings indicate strong support for legal reform while maintaining constitutional safeguards.

Table 5. Constitutional Protection and Regulatory Approach towards deep fake Technology

S.No	Statement	Agree	Neutral	Disagree
1	Deep fake technology requires stronger constitutional and legal protection mechanisms	94 (75)	16 (13)	15 (12)
2	Unregulated deep fake may seriously affect individual reputation and dignity	99 (79)	14 (11)	12 (10)
3	Strict regulation of deep fake may create concerns relating to freedom of speech	73 (58)	27 (22)	25 (20)
4	Constitutional rights and technological innovation	103 (82)	11 (9)	11 (9)

	must be balanced in Deep fake regulation			
5	Public awareness and legal education are necessary to address Deep fake -related harms	108 (86)	9 (7)	8 (7)

Sources – Primary Data

Interpretation:

Table 5 presents respondents' views regarding constitutional protection and the regulatory approach towards deep fake technology. A majority of respondents, 94 (75%), agree that stronger constitutional and legal safeguards are required to address Deep fake -related harms. 99 respondents (79%) believe that unregulated deep fake can seriously affect reputation, dignity, and personal rights. Further, 73 respondents (58%) agree that strict regulation may raise concerns relating to freedom of speech and expression, indicating the need for careful legal balancing. A significant majority, 103 respondents (82%), support a regulatory framework that balances constitutional rights and technological innovation. Additionally, 108 respondents (86%) agree that public awareness and legal education are important measures for dealing with deep fake harms. These findings show that respondents favour stronger regulation, but also emphasize the importance of maintaining constitutional values and promoting legal awareness.

FINDINGS:

The study shows that 83% of respondents are aware of deep fake technology, indicating growing legal awareness among law students and lawyers. Around 78% believe that deep fake affect constitutional rights such as privacy and dignity, while 74% feel that deep fake pose a threat to democratic integrity and freedom of speech. About 59% consider the existing criminal law framework inadequate to regulate deep fake -related harms, and 65% agree that present laws face difficulties in applying criminal liability to AI-generated content. Nearly 70% state that legal principles such as mens rea and attribution create challenges in deep fake cases, and 73% support legal responsibility of digital platforms for harmful deep fake content. Further, 50% believe that the Information Technology Act, 2000 is not fully effective in dealing with deep fake regulation, while 77% support the need for a separate legal framework. Around 82% agree that regulation should balance constitutional rights with technological innovation. Overall, the findings clearly indicate that deep fake technology creates significant

constitutional and criminal law challenges, and there is strong support for legal reform and a balanced regulatory framework in India.

ANALYTICAL FRAMEWORK OF THE STUDY

CHAPTER – I

1.1 Meaning and Definition of deep fake Technology

Deep fake technology refers to a form of Artificial Intelligence (AI)-generated synthetic media in which digital content such as images, audio recordings, or videos are manipulated or artificially created to make an individual appear to say or do something that never actually occurred. The term "Deep fake" is derived from the combination of the words "deep learning" and "fake". Deep learning refers to a branch of artificial intelligence that enables computer systems to learn patterns from large datasets through layered neural networks, while the term fake denotes fabricated or manipulated content. Through advanced computational techniques, deep fake technology produces highly realistic digital outputs that may be difficult to distinguish from authentic material.

According to Robert Chesney and Danielle Citron, deep fake are "highly realistic fabricated digital media created using artificial intelligence techniques capable of depicting events that never actually happened." The authors observe that deep fake technology has the capacity to influence privacy, democratic institutions, public trust, and national security due to its ability to create convincing false narratives. Their work identifies deep fake as an emerging legal and technological challenge requiring regulatory attention in the digital era.

1.2 Artificial Intelligence, Machine Learning and Synthetic Media

Artificial Intelligence (AI) refers to computer systems that perform tasks requiring human intelligence, such as learning, decision-making, and problem solving. Machine Learning (ML) is a branch of AI that enables systems to learn from data and improve performance without explicit programming. Synthetic media refers to digitally created or AI-manipulated content including images, videos, audio, and text. Deep fake technology functions through these technologies by using AI and machine learning models to generate realistic but artificial digital content.

1.3 History and Evolution of Deep fake Technology

The history of deep fake technology is closely connected with the development of Artificial Intelligence, machine learning, and deep learning technologies. Early forms of digital image and video editing existed before artificial intelligence, but they required manual human editing. With the advancement of AI systems, computers became capable of automatically analysing and reproducing human faces, voices, and expressions using large datasets. The term "Deep fake" became widely known in 2017, when AI-generated face-swapping videos appeared on online platforms. Over time, improvements in deep learning algorithms, neural networks, and generative AI models increased the accuracy and realism of deep fake content. Initially, deep fake were used mainly for entertainment, media production, and digital creativity. However, their growing accessibility and realistic nature have led to misuse in areas such as misinformation, cyber fraud, identity theft, political propaganda, and privacy violations, making deep fake technology a major concern in the digital era.

1.4 Types of Deep fake Technology

Deep fake technology appears in different forms depending upon the nature of the manipulated digital content. The most common forms are image deep fake, video deep fake, audio deep fake, and text-based synthetic content**.**

Image deep fake involve the creation or alteration of photographs using artificial intelligence tools. In this form, facial features, expressions, or identities may be digitally changed to produce realistic but fabricated images. Such manipulated images are often used for impersonation, misinformation, or reputational harm.

Video deep fake are one of the most widely discussed forms of deep fake technology. They involve the use of AI systems to modify facial expressions, speech movements, gestures, or actions in a video recording. Through techniques such as face swapping and digital replacement, a person may appear to speak or act in a manner that never actually occurred. Due to their realistic appearance, video deep fake create concerns relating to political misinformation, fraud, and digital deception.

Audio deep fake refer to AI-generated imitation of a person's voice, tone, pronunciation, and speaking style. By analysing voice samples, machine learning systems can generate artificial

speech closely resembling an individual's original voice. Audio deep fake may be used in entertainment and voice assistance technologies, but they also create risks of fraud, identity theft, and misleading communication.

Text-based synthetic content involves AI-generated written material created through language models and automated systems. Such content may include fabricated messages, articles, online posts, or digital communications designed to imitate human writing patterns. These forms of synthetic media contribute to the spread of misinformation and digital manipulation.

CHAPTER – II

2. Constitutional Challenges and Criminal Liability in the Digital Era

2.1 Deep fake and Constitutional Rights: Privacy, Dignity and Reputation

Deep fake technology creates serious concerns relating to constitutional rights such as privacy, dignity, and reputation in the digital era. The use of artificial intelligence to manipulate images, videos, and audio without consent may interfere with an individual's personal autonomy, identity, and informational privacy. Deep fake can falsely portray a person engaging in acts or statements that never actually occurred, thereby causing damage to personal dignity and social standing. The increasing use of synthetic media in online spaces has strengthened concerns regarding digital misuse and constitutional protection.

Under the Constitution of India, the right to privacy and human dignity forms an important part of Article 21, which guarantees the right to life and personal liberty. The misuse of deep fake technology through non-consensual content creation, impersonation, and reputational attacks raises questions regarding protection of individual rights in the digital environment. Deep fake involving fabricated intimate content, false political statements, or manipulated personal images may directly affect a person's dignity, mental well-being, and public reputation.

Further, reputation is recognised as an important constitutional value linked with the right to life and personal liberty. AI-generated false content may lead to defamation, humiliation, and loss of public confidence, particularly when manipulated media is rapidly circulated through digital platforms. Therefore, Deep fake technology presents a significant constitutional

challenge requiring legal safeguards to protect privacy, dignity, and reputation in the modern digital age.

2.2 Freedom of Speech, Democratic Integrity and Digital Manipulation

Deep fake technology raises concerns relating to freedom of speech, democratic integrity, and digital manipulation. Under Article 19(1) (a) of the Constitution of India, citizens have the right to freedom of speech and expression, including digital expression. However, deep fake can be used to spread false information, manipulated political content, and misleading digital media, affecting public opinion and democratic processes. Such content may influence elections, weaken public trust, and promote misinformation. At the same time, regulation of deep fake must balance free speech and reasonable restrictions under Article 19(2). Excessive regulation may affect lawful expression and innovation, while lack of regulation may allow harmful digital misuse. Therefore, deep fake technology creates a challenge between free speech, democratic protection, and digital governance.

2.3 Criminal Liability in AI-Generated Digital Offences

Criminal liability in AI-generated digital offences refers to the legal responsibility arising from the creation, use, or circulation of harmful AI-generated content such as deep fake. Deep fake technology may be used for identity theft, fraud, defamation, cyber harassment, misinformation, and non-consensual content creation. The use of AI in digital offences creates difficulties in identifying the person responsible for the harmful act. Questions arise regarding the liability of the creator, user, or digital platform involved in the production and distribution of deep fake content. Therefore, deep fake technology presents new challenges to traditional principles of criminal law in the digital era.

2.4 Mens Rea and Evidentiary Challenges

Deep fake technology creates challenges relating to mens rea, attribution of liability, and evidentiary authenticity in criminal law. Mens rea, which refers to the guilty intention or mental element of an offence, becomes difficult to determine in AI-generated offences involving automated systems and digital manipulation. Questions often arise regarding whether the criminal intention belongs to the creator, user, programmer, or distributor of the deep fake content.

Attribution of liability is another major concern because identifying the actual person responsible for creating or circulating deep fake is difficult in digital environments. The anonymous and borderless nature of online platforms complicates the process of fixing legal responsibility. Further, deep fake create evidentiary challenges by affecting the authenticity and reliability of digital evidence. Manipulated images, videos, or audio recordings may weaken trust in electronic evidence used in legal proceedings.

2.5 Intermediary Liability and Platform Accountability

Intermediary liability and platform accountability are important issues in the regulation of deep fake technology. Digital platforms and social media intermediaries play a major role in the hosting, sharing, and circulation of AI-generated content. The rapid spread of deep fake videos, images, and audio through online platforms increases concerns regarding the responsibility of intermediaries in preventing harmful digital content.

Platform accountability refers to the duty of digital platforms to adopt reasonable measures for detecting, monitoring, and controlling the misuse of deep fake technology. The failure to address manipulated content may contribute to the spread of misinformation, reputational harm, online harassment, and digital deception. At the same time, imposing excessive responsibility on intermediaries may affect freedom of digital communication and innovation. Therefore, intermediary liability remains an important issue in balancing digital governance, user safety, and responsible platform conduct in the digital era.

CHAPTER – III

3. Legal Framework, Judicial Approach and Regulatory Reform

3.1 Constitutional and Statutory Framework Governing Deep fake in India

In India, there is no separate legislation exclusively regulating deep fake technology. However, constitutional and statutory provisions provide a legal framework for addressing deep fake - related harms. Under the Constitution of India, Article 19(1)(a) guarantees the right to freedom of speech and expression, while Article 19(2) permits reasonable restrictions in the interests of sovereignty, public order, decency, morality, defamation, and incitement to an offence. Further, Article 21, which protects the right to life and personal liberty, includes protection of privacy, dignity, and reputation, rights that may be affected by manipulated digital content.

At the statutory level, the Information Technology Act, 2000 contains important provisions relevant to deep fake offences. Section 66C deals with identity theft, Section 66D addresses cheating by personation through computer resources, and Sections 67 and 67A regulate the publication or transmission of obscene and sexually explicit electronic material. In cases involving fabricated digital content causing reputational or financial harm, these provisions may become applicable.

Further, the Bharatiya Nyaya Sanhita, 2023 contains provisions relating to cheating, forgery, defamation, false electronic records, and offences affecting reputation and public trust, which may apply to harmful uses of deep fake technology. Thus, the existing constitutional and statutory framework provides partial regulation of deep fake harms, although India presently lacks a dedicated legal regime specifically addressing AI-generated synthetic media.

3.2 Information Technology Act, 2000 and Bharatiya Nyaya Sanhita, 2023

The Information Technology Act, 2000 provides legal provisions dealing with offences committed through computer systems and electronic communication. Section 66C punishes identity theft, including the fraudulent use of another person's electronic signature, password, or unique identification information. This provision becomes relevant where deep fake technology is used to imitate or misuse a person's digital identity. Section 66D deals with cheating by personation using computer resources, where digital platforms or electronic communication are used to deceive another person for wrongful gain or harm. Further, Section 67 prohibits the publication or transmission of obscene material in electronic form, while Section 67A specifically regulates sexually explicit electronic content, provisions which may become applicable in cases involving deep fake pornography or manipulated intimate content.

The Bharatiya Nyaya Sanhita, 2023 also contains provisions relevant to deep fake -related offences. The Act criminalises offences such as cheating, forgery, defamation, and falsification of electronic records. Where deep fake technology is used to create false representations, damage reputation, deceive individuals, or produce fabricated digital content, these criminal provisions may be invoked depending upon the nature of the act and the resulting harm. Thus, both the Information Technology Act, 2000 and the Bharatiya Nyaya Sanhita, 2023 form an important part of the existing legal response to digital offences involving Deep fake technology.

3.3 Judicial Approach and Important Case Law Analysis

(i) Justice K.S. Puttaswamy v. Union of India (2017)

In Justice K.S. Puttaswamy v. Union of India *(2017),* the Supreme Court of India recognised the right to privacy as a fundamental right under Article 21 of the Constitution. The Court held that privacy forms an essential part of life, liberty, dignity, and personal autonomy. This judgment is important in the context of deep fake technology because AI-generated manipulation of images, videos, and personal data without consent may interfere with an individual's privacy and dignity. The case establishes constitutional protection against unlawful digital intrusion and misuse of personal identity.

(ii) Shreya Singhal v. Union of India (2015)

In Shreya Singhal v. Union of India (2015), the Supreme Court struck down Section 66A of the Information Technology Act, 2000 as unconstitutional for violating freedom of speech and expression under Article 19(1)(a). The Court held that vague restrictions on online speech may have a chilling effect on free expression. The judgment is relevant to Deep fake regulation because any legal framework governing synthetic media must balance digital free speech and constitutional restrictions under Article 19(2).

(iii) Subramanian Swamy v. Union of India (2016)

In Subramanian Swamy v. Union of India (2016), the Supreme Court upheld the constitutional validity of criminal defamation provisions under the Indian Penal Code. The Court observed that reputation is an important part of the right to life under Article 21. This principle has direct relevance to deep fake technology because fabricated digital content may damage a person's image, reputation, and social standing through false statements, manipulated videos, or synthetic media.

(iv) Anvar P.V. v. P.K. Basheer (2014)

In Anvar P.V. v. P.K. Basheer (2014), the Supreme Court clarified the legal position regarding electronic evidence. The Court held that electronic records must satisfy statutory requirements for admissibility and proof in legal proceedings. This decision is significant in relation to deep fake technology because manipulated videos, audio recordings, and digital images raise

concerns regarding the authenticity, reliability, and evidentiary value of electronic material before courts.

3.4 Comparative Legal Approaches towards deep fake Regulation

Different countries have adopted different approaches for regulating Deep fake technology depending upon their legal and policy priorities.

The United States follows a sector-specific and decentralised approach. Instead of a single comprehensive deep fake law, regulation mainly exists through state laws, election rules, privacy protections, and platform liability measures. The U.S. approach places strong emphasis on freedom of speech, innovation, and protection against harmful impersonation and non-consensual synthetic content. Recent policy discussions and federal measures have focused on AI-generated intimate imagery, election misinformation, and disclosure obligations.

The European Union adopts a risk-based regulatory model under the AI Act (Regulation (EU) 2024/1689). The EU framework requires transparency obligations for AI systems generating synthetic or manipulated content, including deep fake. Providers and users must disclose or label AI-generated content where required. The European approach mainly focuses on fundamental rights, trustworthy AI, safety, transparency, and accountability.

China follows a comparatively strict and centralised regulatory approach towards deep fake and synthetic media. China's Deep Synthesis Provisions require providers to implement measures such as content labelling, identity verification, consent mechanisms, and prevention of misleading or unlawful synthetic content. The regulatory model emphasises public order, information control, and platform compliance in the governance of AI-generated media.

These comparative approaches show that while the United States prioritises speech and innovation, the European Union emphasises risk-based transparency and fundamental rights, and China adopts stronger regulatory control and compliance requirements for deep fake governance. Such international developments provide useful lessons for strengthening the Indian legal framework.

LIMITATION OF THE STUDY:

The present study is subject to certain limitations. The empirical research is confined to the

Chennai area and is based on responses collected from 125 respondents consisting of law students and lawyers. Therefore, the findings may not represent the opinions of the entire population or other geographical regions of India. The study is limited by time, accessibility of respondents, and availability of data relating to deep fake technology. Further, the research mainly focuses on the constitutional and criminal law dimensions of deep fake technology and does not extensively examine technical or software engineering aspects of AI systems. Since deep fake regulation is an emerging area, the study is also limited by the absence of a dedicated legal framework and limited Indian judicial precedents on the subject.

SUGGESTIONS:

India should enact a dedicated deep fake Prevention and Accountability Act establishing a National Deep fake Emergency Response Cell with powers for real-time detection, digital tracing, and immediate intervention. A one-click cyber complaint portal should enable instant victim reporting, automatic case registration, and temporary blocking of harmful content. The law should guarantee strict confidentiality of victim identity and digital records. Mandatory AI watermarking and authenticity labels should be imposed on all synthetic media. Social media platforms must implement continuous deep fake monitoring and cooperate with government detection systems. Special fast-track cyber courts should ensure speedy investigation, prompt it content removal, and effective criminal action against offenders. A national public verification platform may be established to allow users to instantly verify the authenticity of viral audio, video, and image content. Repeat offenders and organised creators of malicious deep fake should face enhanced penalties, including long-term platform restrictions and financial liability for damages caused. Cross-border cooperation mechanisms should also be strengthened to address deep fake originating from foreign jurisdictions and ensure effective international enforcement. Furthermore, victims of malicious deep fake should be provided with comprehensive psychological support through free counseling services, mental health assistance, and rehabilitation programmes to address emotional distress, reputational harm, and social consequences arising from deep fake victimization.

CONCLUSION:

Deep fake technology represents one of the most significant challenges of the modern digital era, where the rapid growth of artificial intelligence has blurred the line between reality and fabrication. While deep fake offer opportunities for innovation, creativity, and technological

development, their misuse creates serious concerns relating to privacy, dignity, freedom of speech, democratic integrity, and criminal accountability. The study reveals that the existing Indian legal framework provides only limited protection and lacks a specialised mechanism to address AI-generated harms effectively. Issues relating to criminal liability, evidentiary authenticity, platform responsibility, and victim protection demand urgent legal attention. In a technology-driven society, regulation cannot rely solely on traditional legal principles; it must evolve with emerging digital risks. Therefore, India requires a balanced, future-oriented, and rights-based regulatory approach that safeguards constitutional values while promoting responsible technological advancement. Effective governance of deep fake technology is not merely a legal necessity but an essential step towards preserving truth, trust, and justice in the contemporary digital age.

REFERENCES:

BOOKS:

1. M.P. Jain, Indian Constitutional Law, 9th edn., LexisNexis, Haryana, 2018, pp. 1089–1105, 1223–1245.

2. Dr. J.N. Pandey, The Constitutional Law of India, 60th edn., Central Law Agency, Allahabad, 2023, pp. 135–146, 181–188.

3. Durga Das Basu, Introduction to the Constitution of India, 26th edn., LexisNexis, Haryana, 2021, pp. 238–245, 267–281.

4. Justice Yatindra Singh, Cyber Laws, Universal Law Publishing, New Delhi, 2012, pp. 185–210.

5. Dr. Farooq Ahmad, Cyber Law in India: Law on Internet, 5th edn., Pioneer Books, New Delhi, 2018, pp. 96–109.

JOURNALS & ARTICLES:

6. Danielle Keats Citron & Robert Chesney, "Deep fake : A Looming Challenge for Privacy, Democracy, and National Security", 107 California Law Review (2019), pp. 1753–1820.

7. Ian Goodfellow et al., "Generative Adversarial Networks", Advances in Neural Information Processing Systems, Vol. 27, 2014, pp. 2672–2680.

8. Hany Farid, "Fake Photos and Videos are a Growing Threat", Issues in Science and Technology, Vol. 35, No.1, 2018, pp. 47–50.

9. Jack M. Balkin, "Free Speech in the Algorithmic Society: Big Data, Private Governance and New School Speech Regulation", 51 UC Davis Law Review (2018), pp. 1149–1210.

10. Anita L. Allen, "Coercing Privacy", 40 William & Mary Law Review (1999), pp. 723–757.

GOVERNMENT REPORTS:

11. NITI Aayog, National Strategy for Artificial Intelligence – #AIForAll, Government of India, 2018, pp. 12–15, 34–41.

12. Ministry of Electronics and Information Technology (MeitY), Report of the Committee on Digital Governance and Artificial Intelligence Policy Discussions, Government of

India, relevant policy materials.

13. OECD, OECD Recommendation of the Council on Artificial Intelligence, Organisation for Economic Co-operation and Development, Paris, 2019, pp. 7–9.

14. European Union, Regulation (EU) 2024/1689 — Artificial Intelligence Act, European Parliament & Council, 2024.

15. Cyberspace Administration of China, Provisions on the Administration of Deep Synthesis of Internet Information Services, China, 2022–2023.

STATUTORY PROVISIONS:

16. The Constitution of India, 1950

    - Article 14
    - Article 19(1)(a)
    - Article 19(2)
    - Article 21

17. The Information Technology Act, 2000 (Act No. 21 of 2000)

    - Section 66C – Identity Theft
    - Section 66D – Cheating by Personation by using Computer Resources
    - Section 67 – Obscene Material in Electronic Form
    - Section 67A – Sexually Explicit Electronic Content

18. The Bharatiya Nyaya Sanhita, 2023

    Relevant provisions relating to Cheating, Forgery, Defamation, False Electronic Records

19. The Bharatiya Sakshya Adhiniyam, 2023

    Provisions relating to Electronic Records and Digital Evidence

CASE LAW CITATIONS:

20. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

21. Shreya Singhal v. Union of India, (2015) 5 SCC 1.

22. Subramanian Swamy v. Union of India, (2016) 7 SCC 221.

23. Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.

WEB SOURCES:

JOURNAL:

24. https://www.californialawreview.org/print/deep-fakes-a-looming-challenge-for-privacy-democracy-and-national-security/

25. https://papers.nips.cc/paper/2014/hash/f033ed80deb0234979a61f95710dbe25-Abstract.html

26. https://repository.law.upenn.edu/Documents/Detail/400797?item=489788

27. https://lawreview.law.ucdavis.edu/sites/g/files/dgvnsk15026/files/media/documents/51-3_Balkin.pdf

GOVERNMENT REPORTS:

28. https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf

29. https://www.niti.gov.in/sites/default/files/2021-02/Responsible-AI-22022021.pdf

30. https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449

31. https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

32. https://www.chinalawvision.com/2025/02/digital-economy-ai/deep-synthesis-not