International Journal of Science, Strategic Management and Technology
Volume **02** Issue **05** May-**2026** | ISSN: **3108-1762 (Online)** | Impact Factor: 3.8
An International, Peer-Reviewed, Open Access Scholarly Journal Indexed in recognized academic databases

The Legal Aspect of Deep-Fake: Blurring the Line Between Reality and Illusion

Adv. Himangana Priya

https://doi.org/10.55041/ijsmt.v2i5.351

Cite this Article: Priya, A. H. (2026). The Legal Aspect of Deep-Fake: Blurring the Line Between Reality and Illusion. International Journal of Science, Strategic Management and Technology, *02*(05). https://doi.org/10.55041/ijsmt.v2i5.351

CHAPTER 1
i.INTRODUCTION

As we all know, that the technology has evolved to a very large extent, which ultimately led to the evolution of AI, now with the help of AI and machine learning, the concept of "DEEPFAKES" arose. Deep-fake is the technology of generating synthetic media in which a person's voice or likeness is substituted by fake ones. Like every coin has two faces, the use of Deep-fake is also classified into two types:

1 Positive use
2 Malicious use

In the field of education, entertainment industry, business etc. it is often used in a positive manner. But, when it is used maliciously it jeopardizes people's rights and social confidence. Defamation, financial fraud, political deception and non-consensual pornography are some of the examples of the malicious use of deep-fakes.

This study investigates the significant ethical and legal issues raised by deep-fake, looking at how this technology obfuscates the distinction between the reality and illusion [fake ones], the integrity of democratic states can be compromised by it as well as it can endanger the Intellectual property rights, and the fundamental right to privacy of the people.

1.1 BACKGROUND AND EVOLUTION OF DEEPFAKE TECHNOLOGY

The term "deep-fake" is made up of the combination of two different words; i.e. "deep-learning" + "fake", they both together form the phrase "Deep-fake", which is becoming more than just a technological curiosity. It is also causing a serious threat to the ideas of truth and digital identity. It started in Reddit's virtual hallway in the year of 2017 only rather than created in a lab. The ideas of editing the photos, videos etc. are not a new concept, but the extent had enlarged due to the deep-fake technology. Majorly, the use of AI for generating deep-fake substances started in the post COVID era, i.e. after the year 2020-2022, mostly we can say from the year 2024. Till date the corporate companies as well as the normal individuals are having lack of technical defences to cope against deep-fakes and other AI based technological threats.

In today's era, the social-media platforms like the Facebook, X, YouTube etc. are being used by millions of users for the source of entertainment, news and learning different skills, also, due to the digital India movement, the number of people using the technology had grown rapidly. But, the news, the photos, videos etc. we are watching is original or not is a major concern; if the content is fake then it will cause a negative impact on the knowledge as well as the decision making power of the individuals.

Recent technical developments have made it simple to produce what are now known as "deep-fakes," which are extremely lifelike films with minimal evidence of manipulation.
Artificial intelligence (AI) programs that blend, merge, replace, and superimpose photos and video clips to produce phony videos that look real are known as deep-fakes. Without the approval of the individual whose image and voice are used, deep-fake technology can create, for instance, a hilarious, pornographic, or political video of someone saying anything.

The scope, scale, and sophistication of the technology involved in deep-fakes are revolutionary because nearly anyone with a computer can create phony films that are nearly identical to real media.
In the future, deep-fakes will probably be used more frequently for revenge porn, bullying, fake video evidence in court, political sabotage, terrorist propaganda, blackmail, market manipulation, and fake news, even though early examples of deep-fakes focused on political figures, actresses, comedians, and entertainers having their faces woven into porn videos.

1.1.1 The Historical Context

Photo editing was a time-consuming, manual procedure prior to the digital era. Since, our childhood we had seen movies like Jurrasic Park, The Mummy, Harry Potter etc. which were made with the technology of high end computer generated imagery [CGI] in the era of 1990s and early 2000s, here, the production charges were very high due to the technology used and the procedure was time-taking also.

After the developments of 1990s and 2010s, the new concept of machine learning was introduced in the year 2014, known as “GAN”, i.e. Generative Adversarial Network. It was developed by Ian Goodfellow along with his team. By letting machines to produce images, video, and audio that are considerably more lifelike than anything before possible, GANs paved the way for a new era of synthetic media. This innovation was used in almost all early deep-fake systems.
Although CGI has been used for digital manipulation since the 1990s, the REDDIT "deep-fakes" event in 2017 upped the game by automating the production of sexual, non-consensual content. The transition from celebrity parodies to sophisticated political disinformation and financial fraud has happened quite quickly in India. So, 2017 can be called as the year which brought the regular users in the dark world of technology, where the users started using technologies outside the ambit of academic uses. At this time, the technology was fuelling on the both sides, i.e. for the creativity as well as for the harmful misuse, including the non-consensual pornography. There were some open sources tool like DEEPFACELAB which were used as a platform. Thus, in order to identify the fake content before it spreads, necessity for the protection arose.
Now, in today’s digital era, the use of deep-fakes is not only limited to the negative impact like fraud, impersonation etc. it is now used in the legitimate purpose of education, media etc.

1.1.2 The Transformation:

In the earlier times, to do the certain edits, professionals were required along with high end computer system, which is drastically changed in today’s era, where a simple computer can perform the same task without any-kind of professional knowledge of the user. The reasons that led to the development are as follows:
The 1st reason was the development of the technology like GPUs, i.e. Graphic Processing Unit. For example:-Hardware acceleration.

The 2nd main reason was the access to large data, i.e. today billions of photos and videos can be accessible by the user through the medium of internet.

The 3rd major reason was the development of the technology like Generative Adversarial Networks.

The transformation has happened quickly in the Indian setting. Technology has advanced more quickly than the legal framework, from beginning of face-swapping applications used for amusement to the more recent and alarming use of synthetic media in political campaigning and non-consensual explicit content.

1.1.3 The India-Specific Evolution

Due to low digital literacy in rural areas and strong smartphone usage, the Indian digital environment is distinct. As a result, deep-fake have become "viral" before they can be independently validated. The Indian government announced the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026 as a result of historic events like the Rashmika Mandanna’s deep-fake case in 2024. The first official legal definition of "Synthetically Generated Information" (SGI) is currently provided under these regulations.

1.2 The Process of Generating Synthetic Media:

The process through which the synthetic media of deep-fakes is generated should be known to understand the legal consequences, outcomes, or offshoots of the specific action. The GANs, i.e. Generative Adversarial Network is the tool which is used to produce the majority of high-quality synthetic media.

The Mechanism showing the work of GANs:

The Two-Actor Model

The Generator: An algorithm that uses a training dataset of actual photos to produce phony content (audio, video, or photographs) produces a phony image with the most realistic appearance. Its initial attempts are clumsy and appear to be digital noise.

The Discriminator: An algorithm that serves as a reviewer, trying to discern between "fake" and "real." It detects the fake with ease and provides "feedback" to the Generator.

The Generator eventually creates a "perfect fake" that the Discriminator is unable to identify as these two networks compete. This feedback is used by the Generator to make its next try better. Until the Discriminator is unable to discern between the real and fake photos, this cycle is repeated thousands of times.

Legal Significance of the Mechanism

Because of its "adversarial" nature, the software is made to evade detection. This makes it challenging for the Indian justice to rely only on "visual inspection" as evidence in court, creating a "cat-and-mouse" game for digital forensics.

Emerging Technologies

By 2026, voice cloning and diffusion models will have joined GANs as the main tools. According to Rule 3[3][a][ii] of the IT Rules, 2026, Indian law now requires such material to have "Provenance Metadata" a digital fingerprint that links the file to the particular AI tool that created it.

The Live Generation of Images and Voices:

It is the newest from of fraud taking place with the help of AI, in this type of crime the fraudster generate the images and voice of the people known to the victim during live video calls, thus the victim believes the fraudsters and then, they target the victim. Earlier, the fraudsters were using only the voice-calls to scam the victim, which has now changed to the video-calls etc.

Now, due to the rise in this type of generation of synthetic media, no any industry is safe from it, they must be ready for the upcoming threats due to this Deep-Fake technology.

1.3 A Brief overview of the current Indian legal system:

Under the provisions of IT Act 2000, there are some sections which helps in tackling few kinds of problems related to the digital world, i.e. section 66E, section 67, section 67A etc. helps the victim in case of circulation of the images, videos etc. of them without their consent, also section 67B, specifies the punishment for publishing, transmitting materials related to the child-pornography.

Also under BNS, 2023, there are few sections which guards the rights of the victims like section 77, section 356 and section 351.

Now, under the DPDP Act, 2023, the rules regarding the rights related to the individuals whom data is being used as well as the reason for why that particular data is being used is laid down, known as the “Rights of Data Principles”.

Examples of few Case laws:

Anil Kapoor v. Simply Life India & Ors. (2023 SCC Online Del 5914)

Legal Principle: The Delhi High Court established a precedent for celebrity protection by defending the actor's "Personality Rights" against AI-generated "likeness" and voice clones.

Shilpa Shetty Kundra v. Getoutlive.in (2025 SCC Online Bombay 5486)

Legal Principle: The Bombay High Court ruled that AI content that violates people's dignity violates their right to privacy under Article 21 and ordered the immediate removal of deep-fakes.

Nandamuri Taraka Rama Rao v. Ashok Kumar (2025 SCC Online Del 9417)

Legal Principle: Safeguarded Junior NTR's "Personality Rights" from unapproved AI-generated commercial goods.

Cognizance of False Verdicts by the Supreme Court (Order dated February 27, 2026) The Supreme Court ruled that using AI-generated "fake judgments" that is, cases that don't exist in a trial court constitutes professional misconduct and jeopardizes the judiciary's legitimacy.

1.4 Constructive Uses vs. Destructive uses of AI generated synthetic content: Deep-fakes.

The use of deep-fake is not only limited to the negative side. Like every coin has two faces, the use of deep-fake can also be categorised into two types i.e. the positive use and the malicious use. Now, it depends upon the will of the user to use positively or negatively the technology.

1.4.1 The Constructive use of Deep-fake technology:

The use of deep-fake technology can be done in positive manner also. It is widely used in the entertainment industries, in the educational sector for teaching, healthcare services and also in businesses like e-commerce.

Film Industry:
There is a wide use of Deep-fake in the film industry. As India is a nation where people speaking several languages live together, thus, a single movie made in a particular language can be dubbed into several different languages. Also, there is a system of voice cloning present with the help of AI. Sometimes, few scenes of a movie is edited with the help of deep-fake to avoid the cost of shooting once again. Now, imagine a scenario where an actor dies while shooting for a film, then also we can take help and can generate deep-fake of him to complete the movie.

Education:

Generating live videos of famous historical personalities for the proper visual understanding of the students. For example: Generating the synthetic video of Dr. B.R.Ambedkar teaching the Constitution of India to the students. Language barriers were broken down in a 2019 global malaria awareness campaign featuring David Beckham, who seemed bilingual in an instructional advertisement using speech and visual alteration technology (USAT03). In a similar vein, deep-fake technology can overcome language barriers during video conferences by translating speech and concurrently changing mouth and facial movements to enhance eye contact and give the impression that everyone is speaking-the-same-language.

Societial use and Medical use:

In societal use, one can generate the image/videos of their deceased loved ones to comfort themselves in their absence. Also, as we see till date when the topic is of transgender the society is still somewhere orthodox, thus, most of the transgender are not able to express themselves whole heartedly, now, with the help of deep-fakes they are able to see themselves in their desired gender. In medicinal use, with the help of deep-fake one can generate the voice clones of the people suffering from ALS and had lost their ability to speak.

Business:-

In business, the companies are now generating AI supermodels for cost cutting and those models are becoming popular also. These deep-fake models help the people to look the exact same dress on different colour tones. Also, some e-commerce websites are now generating AI based deep-fake image of the customer to virtually try on the products by themselves for looking into the fitting etc. Again the on-going trend of personal avatar is also generated through deep-fake AI only.

Cultural Preservation:

We can generate images of ancient attires of our earlier generation to visualize them for our better understanding. Also we can generate the images of the monuments which are now majorly destroyed to see how it looked when it was in a good structure. We can restore our old, local folk music and movies.

Sarcasm and Creativity:

Digital artists push the limits of creativity and political parody through the use of synthetic media. Example: Memes made on Indian PM and PM of Italy.

1.4.2 Deconstructive Application of Deep-fakes:

Non-Consensual Intimate Imagery (NCII):

Deep-fake porn videos are generated by grafting the face of the victim with the body of someone else. According to Article 21 of the Indian Constitution, this constitutes a serious violation of the right to privacy.

Financial Fraud:

AI can be used in causing financial frauds like the Phishing attacks, here the attacker can change his/her voice with the help of AI into the voice of the known person of the victim to get the desired financial transfer.

Political Manipulation:

Deep-fakes have the capacity to agitate the crowd and thus can cause the results of the elections getting hampered because of it, which can be harmful for a delicate democracy like India. It can be done by portraying a leader, saying something he/she never said.

Evidence Tampering:

To get the benefit of "reasonable doubt" the criminals can produce any deep-fake document and can claim it to be authentic. Here, section 336 of BNS helps the victim to fight on the ground of Forgery of the evidence.

1.4.3 Few problems addressed by the Indian legal system:

There are certain problems which can be created by using deep-fake technology, are being addressed by the Indian legal system on different names, some of them are as follows:

Sextortion and publishing and transmitting non-consensual images:

Section 66E of the IT Act, 2000 along with section 67 of the IT helps in tackling these kind of offences. Also, section 77 of BNS, i.e. voyeurism along with section 292 of BNS helps the victim to fight against the crime.

Impersonation & Fraud:

Section 66D of the IT Act (Cheating by personation using computer resource) and the section 319 of BNS (Cheating) helps the victim to fight against the crime.

Rumors causing public mischief:

If any kind of political misinformation or statements, rumours etc. are being published then according to the IT Rules 2026, a 3-hours window for taking down the content is provided. Also section 353 of BNS talks about public-mischief.

Forged evidence produced:

To get the benefit of "reasonable doubt" the criminals can produce any deep-fake document and can claim it to be authentic. Here, section 336 of BNS helps the victim to fight on the ground of Forgery.

1.5 The 2026 Regulatory Paradigm:

The Information Technology Amendment Rules, 2026 shifted the burden of proof.

Mandatory Labelling: If the content is synthetic, a label must be visible on 10% of the display surface.

Identity Disclosure: According to Rule 3(1) (b), platforms are now legally obligated to reveal or to identify of a deep-fake creator of the victim upon request.

Loss of Safe Shelter security of the Intermediaries:

A platform (intermediary) may be sued as the "publisher" of the crime and lose their immunity under Section 79 of the IT Act if they do not delete a reported deep-fake within the allotted two to three hours of the provided timeline.

Below is a detailed breakdown of the 2026 Regulatory Paradigm:

1.5.1 The Statutory Definition of "SGI"

Rule 2[1][wa] of the regulations adds the term "Synthetically Generated Information" (SGI) to the legal language.
Definition: Any information i.e. audio, visual, or audio-visual that has been intentionally or algorithmically produced or altered to look genuine and authentic, making it "indistinguishable" from an actual person or event.

Exclusions: "Good Faith" editing is prudently excluded by the law. Colour correction, noise reduction, and simple video stabilization are examples of routine improvements that are not considered SGI. This shields editors and photographers from needless compliance obligations.

1.5.2 The Reduced timeline for taking down the Windows:

The reduction in the amount of time it takes for intermediaries (like Meta, X, and YouTube) to react to illicit content is the biggest shift. Because these are the platforms which is easily accessible by the public at large. Now, if any kind of synthetic media is circulating on these platforms for a longer duration, then it can create threat of destabilization of law and order in the society. If the synthetic media that had been circulated is about a particular person, it will lead to the damage of his societal image i.e. will lead in defamation of the person at a very large extent. Thus, it was the need of the hour to reduce the timeline for the intermediaries to take down the deep-fake content.

Type of Notice / Content Previous Timeline (2021) / New 2026 Timeline

Court or Government Order / 36 Hours / 3 Hours

Non-Consensual Intimate Imagery (NCII) / 24 Hours / 2 Hours

General Grievances (User Complaints) / 15 Days / 7 Days

Urgent Harm (Impersonation/Misinformation) / 72 Hours / 36 Hours

Legal Note: The goal of the "2-hour rule" for deep-fake pornography is to prevent video from going viral and damaging a victim's reputation before they have a chance to consult a lawyer.

1.5.3 Transparency and Labelling Mandates

The 2026 paradigm places the onus of "truth" on the inventor and the platform.

Visual Labelling: Every visual SGI needs to have a label that is "prominent, easily noticeable, and adequately perceivable." Although a set 10% screen area was proposed in early drafts, the final regulations call for a qualitative threshold of "conspicuous visibility."
A "prominently prefixed audio disclosure" (such as an AI voice stating "The following audio is synthetic" before the clip begins) is required for AI-generated voices.

Attributes [data about data] Inserting:

The Information regarding the original source i.e. the digital fingerprints of the material given should be provided. The clearing of the marks regarding the original source is strictly banned under the new regulations.

1.5.4 Audits required by the Intermediaries [SSMIs]:

The Stricter Due Diligence, i.e. SSMIs is applied to all the platforms having more than 5 million users.
1**. User Declarations**: The platform must inquire, "Is this AI-generated?" when a user uploads material.
2. Technical Verification: Users' honesty is not enough for platforms. To determine whether the content is fake, they must use "reasonable technical measures" (automatic AI detectors).
3. Quarterly Warnings: Intermediaries are required to inform users about the repercussions of producing deep-fakes, such as account termination and identity disclosure to law authorities, every three months (previously every year).

1.5.5 The "Safe Harbour" Pivot

Intermediaries have historically benefited from immunity (Safe Harbour) for user-posted content under Section 79 of the IT Act.
The 2026 Change: If intermediaries do not implement "appropriate technical measures," they will no longer be immune.

The Due-diligence Takedowns:
Here, if the moderator of any social media platform, while managing the platform finds something suspicious i.e. in her/his sense seems spams or any offensive content, deletes that content in good-faith, is shielded from any kind of legal action even in absence of a formal court-order.

1.5.6 The revelation of the identity:

If something bad happens to an individual due to the deep-fake, and if he/she requests the intermediary with the help of Rule 3[1][b] of the IT Rules 2026, it is said to provide the information of the creator to the victim or to the law enforcement agencies upon the request. This essentially puts an end to "anonymity" for bad actors that use artificial tools.

ii.TITLE:

LEGAL ASPECTS OF DEEPFAKE: BLURRING THE LINE BETWEEN REALITY AND IILUSION.

LITERATURE REVIEW

The material currently available on deep-fake is divided into three categories: technological, ethical, and legal. The conflict between deep-fake and the right to privacy more especially, the right to be forgotten and the right to publicity is highlighted in legal literature. The authorship and copyright infringement concerns related to AI-generated content based on pre-existing human likenesses are also severely lacking, according to evaluations of recent intellectual property literature. In order to pinpoint the precise statutory gaps in the current legal system I will review IT Act, Intellectual Property laws, a small segment of Constitution law of India.

I. DPDP ACT

So, first of all we will study the newly enacted DPDP Act 2023, in this act it had made compulsory to give the consent for the data which is acquired by the data fiduciary from the one who is generating the data, the data collected must be for a specific purpose, unconditional and free from any kind of ambiguity. Here, the compulsory unconditional consent had made the data of the users vulnerable for the cyber-crimes. The users are not getting the chance for giving their consent according their own will. It is called as the Rights of Data Principal. One of the most famous case, which was happened recently before the act came into force is as follows:

It was made against the policy of sharing the users data is Facebook India Online case, here in this case, the data of the Whatsapp users were shared with the Facebook and if the Whatsapp will not share the data with Facebook, it will lead to the termination of the services. In this case, the honorable Delhi High Court held that this sharing of data is unreasonable and is not fair for the users of Whatsapp. But, in spite of this the policies for the protection of the data, in scenarios like this is not being discouraged by the DPDP Act, and thus, the data shared can be used for various purposes including for AI training also, as the data shared are with the consent of the users only.

I. INFORMATION TECHNOLOGY ACT, 2000.

In India, the act dealing with cyber-crimes is no other than IT Act 2000. The act was influenced by the UNCITRAL Model Law on E-commerce also, the IT Act was amended in the year 2008 due to the emerging cyber-crime threats. But at the time of enactment of the IT Act, it was considered progressive and a kind of ahead of time. There are a lot of cyber related offences which are recognized under the IT Act 2000. They are given under chapter 11 “OFFENCES”. This act covers various kinds of cyber-crimes like, the offence of tampering with the computer related documents, offences related to computer, transmitting obscene material with the help of electronic medium of data transfer.
Now, as we can see that the act came in the year 2000, and at that time AI was not there, as it came before the evolution of AI, machine learning and deep-fake technologies, it lacks in provisions regarding the crimes committed with the help of these new technologies.
The deep-fake cases has an indirect intersection with various crimes like defamation, identity theft, privacy violations, financial scams, sexual harassment etc.
But, in the IT Act the word deep-fake is no-where mentioned. Still it deals with the cases of deep-fakes to a certain extent by the help of various other provisions which are somewhere, indirectly linked with the deep-fake crime. Few examples of these kind of sections are as follows:

i. Identity Theft [section 66C]: It stipulates that anyone who fraudulently or dishonestly uses another person's electronic signature, password, or other distinctive identifying feature faces a maximum sentence of three years in prison and a fine of up to one lakh rupees.

However, it is also unclear if voice cloning and face identity fall under the definition of unique identification

ii. Violation of Privacy [section 66E]: This provision states that anyone who publishes or transmits someone else's private photos without that person's permission is violating that person's right to privacy. The majority of the time, this part is utilized while dealing with altered private photos and videos.

However, it is not made clear in this provision that images or films created with artificial intelligence will fall under its purview.

iii. Transmitting Obscene material in electronic form [section 67 and 67A]: Are used mainly in the cases related to deep-fake pornography.

iv. Controlling Power of the government [section69A]: It authorizes the government that if they think that any content might hamper the sovereignty, national security, public order of a country.

II. THE INTELLECTUAL PROPERTY LAWS

In the Intellectual property laws, there is a concern regarding the authorship of a AI generated content. The acts like the copyright act was made according to the human creativity but today the contents are now being generated by the AI, thus there arises a question regarding the authorship and ownership of the content. The definition of author given under the copyright act is not taking about the AI. So, the programmer, the developer of the platform using AI deep-fake content, the user etc. who is said to be the owner of the content.

Also, there is a concern of copyright infringement happening on the name of training data. Many data which are given to the AI are not given by the consent of the user, they are mostly collected from the online sources without the consent of the user.

III.CONSTITUTIONAL LAW

There are certain articles under the constitution of India, which are majorly being affected by the deep-fake. Especially the right to freedom of speech and expression along with right to privacy are majorly being affected by the deep-fakes. Here, in right to freedom of speech and expression the major challenge is to maintain a balance between speech freedom and it's protection against the digital harm. Like article 19[1][a] protects freedom of speech but does it applies the same way when memes are created with the help of deep-fake and are further being transmitted.

The constitution doesn't clearly talks about right to personality like name, face, voice under the ambit of right to privacy, but the judiciary have gradually recognized it. But, then comes the deep-fake which mostly replicate the individual's replica without his/her consent.

IV. Major Gaps found in the existing laws regarding the deep-fake technology are as follows:

a) There is not any proper dedicated law regarding deep-fake in our country. The IT Act was enacted before the AI was developed thus, it doesn't cover the deep-fake crimes effectively.
b) There is not a properly defined definition of deep-fake which creates gap in the interpretation of the words like deep-fake, synthetic media etc.
c) The present day laws focus on obscenity and impersonation but it don't address the issues like non-consensual AI generated content
d) The liability on the intermediaries is not strict, the platforms don't auto-check the content for removing, it removes the content only when someone raises a complaint.
e) AI labelling should be strictly followed, which is not present effectively today.
f) The jurisdictional challenge in overcoming the cyber-crimes is always present.
g) The data protected is still acting like a myth, biometric data protection rules are somewhere not sufficient enough to protect our data.
h) Political deep-fakes are very much used these days, rules are absent regarding political deep-fakes.
i) The jurisdictional confusion and slow procedure of taking down the content is making the situation worse day by day.
j) Also it is very difficult to know who had created the deep-fake content. There is absence of legislation for the disclosure of the creator with the content.
k) The Intellectual property laws like the copyright act recognizes the modern generative AI system or not is still a question.

P.T.O

iii. STATEMENT OF PROBLEM

Is the current legal frameworks, i.e. tort laws, intellectual property laws, criminal laws, cyber laws etc. are sufficient enough to effectively prevent, identify, punish the circulation of deep-fakes or to address any other kind of challenges created by Deep-fake.

iv. SIGNIFICANCE OF THE RESEARCH

In the present world due to the vast rise in the technology, for the legislators, the courts, and the cyber-security enforcement organizations, it is very important to believe in "seeing is no longer believing". This research will help them to further discuss on the topic of AI regulation by pointing out at the term Deep-fake, which somewhere breaches the fundamental right to life and personal dignity along with other constitutional rights (especially with regard to women's dignity and election integrity). While promoting the technological advancement it helps in creating a road map for constructing a free and fair legal system.

v. SCOPE

This study will focus on the legal consequences of the deep-fake with regard to the right to privacy, defamation, intellectual property rights along with cyber-crimes. It will also examine the international regulations like the EU AI Act along with our legal frameworks like the IT Act 2000, Criminal codes and the DPDP Act.

vi. LIMITATION

As the technology is evolving at a very high speed, the major limitation is that to find out technical findings according to the present needs, as it becomes out of date immediately. Additionally, it is very difficult to provide the remedies regarding the crime related to the technology due to lack of globally accepted legal framework [jurisdiction issues].

P.T.O

vii. OBJECTIVES OF RESEARCH

i. To analyse how the Deep-fake technology is working and the way it is affecting our society and law-order.
ii. To determine whether the dangers created by the deep-fakes could be dealt with our current laws like IT Act, Intellectual Property laws, criminal laws etc. or not.
iii. To evaluate whether our fundamental right to privacy, right to life, right to freedom of speech and expression are balanced or not due to the rise of deep-fakes or synthetic media.
iv. To identify whether the legal, technological and regulatory reformations are needed to stop effectively the malicious use of deep-fakes.

viii. HYPOTHESIS

Due to the rapid evolution and change in the technology and the sudden growth in the number of users, the traditional legal frameworks like the IT act, criminal laws etc. are not alone enough to address the challenges created with the help of AI like the deep-fake. There is an absence of globally accepted legal and regulatory framework could address this issue effectively.

ix. RESEARCH METHEDOLOGY

The study will use empirical research methodology. It will be descriptive and analytical in nature, involving a critical assessment of current laws, legal theories and court rulings.

x. SOURCES OF DATA COLLECTION

Primary Sources: Responses collected with the help of Google forms.

Secondary Sources: Constitution of India, statutory enactments (Information Technology Act, Intellectual Property Laws, Criminal Laws), International treaties, conventions, and landmark judicial pronouncements by Supreme and High Courts. Articles from law journals, reports from Law Commissions and parliamentary committees, news publications.

Tertiary Sources: The articles which are available on online website

P.T.O

xi. CHAPTERIZATION

CHAPTER 1: Introduction

1 The understanding of the term Deep-fake and how it evolved.
1.1 Background and Evolution of Deep-fake Technology.
1.2 Mechanisms of Synthetic Media (GANs - Generative Adversarial Networks).
1.3 A Brief overview of the current Indian legal system.
1.4 Constructive Uses vs. Malicious Applications.
1.5 The 2026 Regulatory Paradigm.
2 TITLE.
3 Literature Review.
4 Statement of Problem.
5 Significance of the research.
6 Scope.
7 Limitation.
8 Objectives of the research.
9 Hypothesis.
10 Research Methodology.
11 Sources of data collection.

CHAPTER 2: Challenges regarding the infringement of Right to privacy and IP in the age of Synthetic Media.

2.1 Infringement of the Right to Privacy and Personal Dignity.
2.1.1 Non-consensual deep-fake pornography and its gendered impact.
2.1.2 Defamation, Identity Theft, and the Right to Publicity. IP challenges in the age of synthetic media

2.3 Copyright Infringement in AI training Data.

2.3.1 Ownership and Authorship of Deep-fake generated context.

2.3.2 The doctrine of "Fair Use" vs. unauthorized digital cloning.

CHAPTER 3: Social impact of Deep-fakes along with International approaches to regulate AI and Intermediaries.

3.1 Social impact of Deep-fakes.

3.2 Analysis of Domestic legal framework and International perspectives: The European Union AI Act, approaches used in USA and UK.

3.3 The role and liability of Intermediaries and Social Media Platforms.

CHAPTER 4: Data analysis.

CHAPTER 5: Conclusion & Suggestion

5.1 Summary of findings.

5.2 Recommendations for legislative amendments and dynamic regulatory models. Also, the need for technological countermeasures (watermarking, AI-detection algorithms) and digital literacy.

CHAPTER 2

CHALLENGES REGARDING THE INFRINGEMENT OF RIGHT TO PRIVACY AND INTELLECTUAL PROPERTY IN THE AGE OF SYNTHETIC MEDIA

2. INTRODUCTION

Artificial intelligence's quick progress has completely changed how information is produced, shared, and used. The rise of "deep-fake" technology is one of the most contentious technological advancements in recent years. Deep-fakes are artificial intelligence-generated or altered synthetic media that mimic real people by employing machine learning and deep learning techniques to produce incredibly lifelike photos, audio files, or videos. Although the technology has valid uses in accessibility, education, entertainment, and digital innovation, its abuse has sparked grave worries about privacy, autonomy, dignity, reputation, and democratic integrity.
Because deep-fakes can cause serious psychological, social, economic, and personal harm, their increasing ubiquity has put judicial systems around the globe under pressure. Deep-fakes, in contrast to conventional image modification techniques, have a sophisticated realism that makes them hard to spot. They can therefore trick viewers into thinking that fake content is real. The protection of the rights to privacy and dignity, which are acknowledged as crucial elements of constitutional and human rights jurisprudence, is significantly impacted by this.

Non-consensual deep-fake pornography, in which a person's face is digitally placed onto sexually explicit content without that person's consent, makes the problem more serious. Women and marginalized groups are disproportionately affected by such usage, highlighting the gendered aspects of technological abuse. Furthermore, deep-fakes enable identity theft, impersonation, defamation, and violations of the right to publicity, all of which jeopardize legal personality and human liberty.

Therefore, the rise of deep-fakes raises important ethical and legal issues, such as whether current laws are sufficient to address harms caused by AI, how to protect privacy and dignity in digital environments, whether consent-based frameworks are adequate, and how to hold creators, distributors, and platforms that enable such content accountable.

2.1INFRINGEMENT OF RIGHT TO PRIVACY AND PERSONAL DIGNITY

It is acknowledged that the right to privacy is a fundamental component of human autonomy and liberty. People may manage personal data, sustain close connections, and protect their identities without unjustified intrusion thanks to privacy.

In the historic decision of Justice K.S. PUTTASWAMY v. UOI (2017), the Supreme Court of India unanimously ruled that the right to privacy is a basic right safeguarded by Article 21 of the Constitution, solidifying the right's constitutional standing. The Court noted that bodily integrity, informational self-determination, decisional autonomy, and the maintenance of one's dignity are all components of privacy.
The ruling acknowledged that privacy and dignity are inextricably linked. Human dignity is the inherent value of every person, necessitating respect for their identity, autonomy, and reputation. An assault on dignity is any misuse of technology that degrades, objectifies, or takes advantage of a person without that person's consent. Because deep-fakes alter and exploit personal information, images, videos, and biometric characteristics, they directly compromise informational privacy. By denying people the ability to decide how their voice or image is utilized, they also violate decisional autonomy.

DEEP-FAKES CAN BE USED AS TOOL FOR INVASION OF PRIVACY

Theft of Personal Information:

Photos, videos, and audio recordings that are either publicly or privately collected are used to construct deep-fakes. Large amounts of personal information are available on social media platforms, which may be used without permission. People frequently become victims just because their photos are available online. Informational privacy is violated when such data

is collected and altered without authorization. People no longer have control over how their personal data is used and distributed.

Consent Violation:
The basis of privacy law is consent. Because deep-fakes are typically produced and disseminated without the subject's consent, they are intrinsically problematic. Until the modified content is extensively disseminated, the victim might not be awarethatitexists.

Deep-fake production becomes a type of digital exploitation when consent is lacking. Consent to share photos does not entail consent to alter them into fake sexual content, even in cases where the original photos were voluntarily posted online.

Psychological and Emotional Damage:
Deep-fake victims frequently experience extreme emotional pain, embarrassment, anxiety, despair, and reputational harm. Because viewers may mistake the phony content for real, the realism of deep-fakes exacerbates these negative effects. Victims of cases with graphic sexual content often face stress, harassment, social exclusion, and career difficulties. The psychological damage brought on by digital humiliation shows how privacy invasions affect people's dignity directly and go beyond information abuse.

An enduring digital footprint:
The durability of internet circulation is one of the main problems caused by deep-fakes. It is almost impossible to remove fake content completely once it has been submitted and spread. Copies may persist on websites, chat apps, and private forums even after platforms remove the content.

Constitutional Dimensions of Deep-fakes

Article 21: Personal Liberty and the Right to Life:

The Right to life and personal liberty is protected under Article 21 of the Indian Constitution. This clause has been interpreted by judges to encompass privacy, dignity, reputation, and mental health. Because deep-fakes violate autonomy and dignity, they are in violation of Article 21. People lose control over their identity and public image when they use non-consensual synthetic media.

Article 19[1][a]: Freedom of Speech and Expression

Concerns about freedom of expression are also raised by deep-fake regulation. Some applications of synthetic media can be classified as political commentary, satire, parody, or creative inventiveness. But the right to free expression is not unqualified. Reasonable limitations in the interests of defamation, decency, morality, public order, and security are allowed under Article 19(2). Therefore, it is possible to control harmful deep-fakes that violate privacy, disseminate false information, or harm one's reputation without violating the rights to free expression guaranteed by the constitution.

Keeping Expression and Privacy in Check:
The difficulty is striking a balance between the rights to privacy and dignity, expressive freedom, and technical progress. While insufficient regulation leaves victims without recourse, excessive control may stifle free speech. Therefore, a proportionality approach that separates malevolent deep-fakes from legal uses must be adopted by courts and legislators.

2.1.1 Non-consensual Deep-fake Pornography and its Gendered Impact

The term "non-consensual deep-fake pornography" describes sexually explicit synthetic media in which a person's body or face is digitally incorporated into pornographic material without that person's agreement. Such material gives the impression that the victim engaged in sexual activity.

This type of misuse is among the most pervasive and detrimental uses of deep-fake technology. According to studies, women are the focus of the vast majority of deep-fake pornography.
Non-consensual deep-fake pornography causes more harm than only reputational injury. It is a serious breach of bodily and informational autonomy as well as sexual exploitation, cyberbullying, and gender-based abuse.

Targeting Women Disproportionately:

According to research, deep-fake pornography primarily targets women. Targets have included journalists, politicians, students, activists, celebrities, and regular ladies.
Deep-fake abuse's gendered component is a reflection of larger patriarchal societal trends. Misogyny, objectification, and sexual dominance are replicated in digital environments through use of the technology. Women are more susceptible to reputational damage from fake sexual content because they are frequently subjected to more scrutiny over sexuality and morals.

Digital Violence and Cyber Misogyny:

Cyber misogyny and deep-fake pornography are closely related. It normalizes online harassment and perpetuates negative preconceptions that reduce women to sexual objects.
Trolling, threats, extortion, and public humiliation are commonplace for victims. Because the abuse is digital, the offenders can target victims anonymously and quickly disseminate content throughout the world.

Chilling Impact on Women's Involvement:

Women are deterred from freely engaging in public life, politics, activism, and internet platforms by the possibility of deep-fake abuse. Due of the ease with which publicly accessible photographs can be altered, women who maintain a public presence are particularly vulnerable. This has a chilling impact on democratic participation and freedom of expression.

Sexually explicit deep-fakes aimed at undermining credibility and silencing voices have increasingly targeted female politicians and journalists.

Sexual Autonomy and Bodily Integrity Violations:

As because it creates sexual behaviour without consent, non-consensual deep-fake pornography compromises sexual autonomy. Digital appropriation of the victim's identity and body occurs for the purpose of sexual exploitation. The violation is psychologically and socially similar to sexual abuse, even if there may not be an actual sexual act. Physical contact is only one aspect of the idea of bodily integrity. Courts are beginning to acknowledge that equally serious suffering can result from digital abuses of sexuality and autonomy.

Social and Psychological Effects on Victims:

Victims frequently encounter humiliation and shame, depression and anxiety, fear of being judged by others, academic and professional repercussions, Break-down in relationships, emotional trauma and suicidal thoughts. Because of patriarchal societal standards, women are disproportionately affected by the social stigma associated with sexual material. Victims may still experience mistrust and moral policing even when content is shown to be fraudulent.

Because victims are unable to completely remove the fake content, the enduring nature of online circulation exacerbates psychological distress.

Sexual Violence with Deep-fake Pornography:

Many academics contend that deep-fake pornography that is not consented to should be classified as sexual violence. Physical assault is not the only kind of sexual violence. It encompasses actions that violate sexual autonomy and dignity, such as coercion or exploitation.

Victims of deep-fake pornography face unwelcoming objectification and public exposure. The severity of the injury is not lessened by the lack of physical contact.
Therefore, it is possible to conceptualize the production and dissemination of such content as image-based sexual assault.

Revenge Pornography:

Deep-fake pornography is comparable to revenge pornography in that both involve the distribution of private photos without permission. Deep-fake pornography, on the other hand, is different since the pictures may be completely fake. Because offenders can avoid responsibility by claiming that the content is not "real," this presents special legal issues. Even when the content is fake, the harm that results is nonetheless real.

2.1.2 DEFAMATION, IDENTITY THEFT AND RIGHT TO PUBLICITY.

Defamation and Deep-fakes:

The publication of untrue remarks that damage someone's reputation is referred to as defamation. Reputation is acknowledged as a crucial component of personal autonomy and dignity. Because fraudulent audio-visual information looks so real, deep-fakes raise special defamation issues. Deep-fake videos, in contrast to textual rumours or photo-shopped images, can accurately show people acting in ways they never did. Also, the viewers are more likely to accept audio-visual evidence, this realism exacerbates reputational loss.

Typically, a defamatory deep-fake involves:
False representation, dissemination or publication, reputational damage, and victim identification. Because deep-fakes inaccurately depict people in compromising, illegal, immoral, or degrading circumstances, they satisfy these requirements.

Examples consist of: Politicians who seem to make provocative remarks, celebrities in pornographic material, businesspeople are shown committing fraud, journalists seen advocating misleading information. Such false representations undermine credibility and public trust.

Constitutional Reputation Protection:

Reputation is acknowledged by Indian courts as a component of Article 21. The Supreme Court stated that reputation is a crucial component of dignity and upheld criminal defamation legislation in SUBRAMANIAN SWAMY v. UOI (2016). Because deep-fakes allow for the broad distribution of fake, defamatory content, they pose a threat to constitutional safeguards.

Challenges in Defamation Law

Dissemination Speed: Before victims can react, deep-fakes can spread quickly thanks to digital platforms.

Anonymity: Criminals may utilize foreign servers, encrypted services, or anonymous accounts.

Proof and Authenticity: When technological know-how is needed, victims may find it challenging to demonstrate manipulation.

Viral Damage: Reputation can be severely harmed by even brief circulation.

Political Deep-fakes and Democratic Damage: Democratic systems are likewise at risk from deep-fakes. It is possible for political people to be erroneously portrayed as saying hurtful things, encouraging violence, or acknowledging corruption. Elections and public opinion can be distorted by such manipulation. Deep-fakes also contribute to a "liar's dividend,"

which allows real evidence to be written off as fraudulent. Public confidence in the media and democratic institutions is weakened by this.

Identity Theft with Deep-fakes:

The unlawful use of another person's identity for dishonest or fraudulent purposes is known as identity theft. Because AI can accurately mimic face characteristics, speech, and behaviours, deep-fakes exacerbate identity theft. Fraudsters can trick family members, employers, or financial institutions by using voice cloning technologies to mimic speech patterns.

Types of Deep-fake Identity Theft

Financial Deception: Fraudsters may pose as CEOs and approve financial transactions by using voice or video clones.

The use of social engineering: Victims may be tricked into disclosing private information by AI-generated mimicry.

Online Deception and Cat-fishing: Deep-fakes can be used to fabricate online personas for extortion or exploitation.

False Endorsements: Influencers and celebrities may be misrepresented as supporting goods or political agendas.

The Law Concerning Identity Theft:

Identity theft including the illicit use of passwords, electronic signatures, or other identifying characteristics is illegal under Section 66C of the Information Technology Act.
Cheating by personation using computer resources is punishable under Section 66D.
However, sophisticated AI impersonation may not be adequately addressed by current regulations.

RIGHT TO PUBLICITY:

The right to regulate the commercial use of one's name, likeness, voice, image, or identity is known as the right to publicity.

For public people, athletes, performers, and celebrities whose identities have commercial worth, this privilege is especially important.

When someone's likeness is utilized for profit without their permission, deep-fake violate their right to publicity.

Examples consist of: Celebrity-starring AI-generated ads, artificial endorsements, digital personas that mimic public figures, videos that have been altered for financial gain.

Differentiating between Rights to Privacy and Publicity:

Publicity and privacy rights are related, yet they are not the same.
People are shielded from unwelcome interference and psychological damage by privacy.
The commercial exploitation of identity and economic interests are the main emphasis of publicity right. Thus, both rights may be violated concurrently by a deep-fake.
For instance, the unapproved use of a celebrity's image in explicit AI-generated content may result in both financial loss and psychological pain.

AI-Based Commercial Exploitation: Synthetic endorsements and AI-generated ads present new legal challenges. Without authorization, a business may utilize AI to replicate a celebrity's image. Customers may be misled by such use, and people may lose out on licensing income.

2.2.2 IP CHALLENGES IN THE AGE OF SYNTHETIC MEDIA AND COPYRIGHT INFRINGEMENT IN AI TRAINING DATA

Intellectual property (IP) law is one of the main fields impacted by deep-fake technology. Conventional IP frameworks were developed for works created by humans and traditional copying methods. AI-generated and AI-manipulated content, however, calls into question these presumptions. Ownership, authorship, copyright infringement, moral rights, fair use, licensing, and digital personality rights are among the issues that come up. The line between inspiration and illegal copying has become more clouded due to AI systems' growing capacity to mimic artistic styles, voices, and likenesses.

Deep-fakes also bring up more general social issues. They have the ability to disseminate false information, influence elections, harm people's reputations, and take advantage of people without their permission. Unauthorized digital clones of actors and singers pose a threat to the entertainment sector, as publishers and artists contest the use of copyrighted content in AI training datasets. Globally, governments and courts are currently finding it difficult to modify current legal theories to fit the quickly developing AI ecosystem.

Four major legal and intellectual property issues associated with synthetic media and deep-fake technologies:

1. IP challenges in the age of synthetic media
2. Copyright infringement in AI training data
3. Ownership and authorship of deep-fake generated content
4. The doctrine of fair use versus unauthorized digital cloning

- **IP Challenges in the Age of Synthetic Media (Deep-fakes)**

Because deep-fake technology makes it possible to replicate and imitate protected content with great realism and little effort, it has raised significant intellectual property problems.

Traditional Intellectual Property Frameworks Face Challenges:

The development of traditional intellectual property laws was predicated on the idea that identifiable human creators are the source of creative works. Because AI systems may independently produce realistic material based on pre-existing works, deep-fake technology challenges this idea.

The main IP issues are as follows: Unauthorized duplication of works protected by copyright, digital voice and likeness cloning, producing derivative works without authorization, ownership and liability are difficult to determine, infringement of one's personality rights, conflicts between jurisdictions across borders.

When it comes to machine-generated innovation, these problems highlight the shortcomings of traditional copyright concepts.

Copyright Challenges:

Unauthorized Duplication:

Copyrighted content, including movies, songs, images, paintings, and written texts, is frequently used by deep-fake systems. Large amounts of internet data are scraped by AI engineers in order to train models. Copyrighted materials may be unlawfully copied, stored, and examined during this procedure.

This puts creators' rights and AI advancement at odds. Because their works are copied digitally, copyright holders contend that using their creations for AI training without permission constitutes infringement. However, AI companies argue that because the process is transformative, it is permitted under principles like fair use or text-and-data mining exclusions.
P.T.O

Derivative Operations.

Content that closely resembles authentic copyrighted works can be produced with deep-fakes. For instance: Songs produced by AI could mimic the voice and style of a vocalist, artificial art may imitate the visual methods used by an artist, texts produced by AI could imitate a writer's style. If these outputs significantly replicate protected expression, they may be considered unapproved derivative works under copyright law.

Challenges with Trademarks and Brands.

Additionally, trademark rights may be violated by synthetic media. Fake celebrity endorsements or AI-generated ads could misrepresent a brand's affiliation. Deep-fakes have the potential to produce fake advertising campaigns that undermine customer confidence.
For example: A deep-fake video can purport to show a famous person promoting a product, artificial influencers could mimic current brand advocates, stock markets may be manipulated by phony business announcements.
Traditionally, customers are shielded from misunderstanding about the source of products and services by trademark law. However, identifying culpability and purpose is made more difficult by AI-generated impersonations.

Rights to Publicity and Personality.
The personality rights, particularly the right to publicity and image rights, are seriously threatened by deep-fake technology. These rights prevent unapproved commercial exploitation of a person's name, voice, appearance, likeness, and identity.
Because AI systems may digitally replicate their voice or appearance without permission, actors, singers, sportsmen, and influencers are especially vulnerable.

Examples consist of songs produced by AI that imitate well-known singers, celebrity likenesses used in artificial advertising, human performers are being replaced by virtual actors. Such actions could circumvent license agreements and profitably exploit an individual's identify.

Moral Rights Issues
Numerous legal systems acknowledge moral rights, such as the attributional right, the right to the work's integrity. Deep-fakes have the potential to harm an artist's reputation by manipulating or distorting their work. An AI system might, for instance, create offensive copies of artistic works or change sequences created by filmmakers.
The creator may no longer have control over how their work is displayed to the public, which makes this problematic.

Enforcement and Jurisdictional Challenges.
Because synthetic media travels the world via the internet, policing is challenging. A deep-fake hosted on servers in one nation may target people in another. Different nations take different stances on copyright legislation, data security, the rights of personality and regulation of AI. Because of this, victims frequently encounter procedural barriers when attempting to get remedies.

Evidentiary Issues.
Digital evidence is undermined by deep-fakes. Digital photos, audio files, and video footage are being used by courts more and more. However, it is challenging to assess authenticity in synthetic media. This leads to difficulties in Criminal actions, Cases of defamation, the integrity of elections, the security of the country. Researchers stress that increasingly complex generation techniques are a persistent threat to deep-fake detection algorithms.

COPYRIGHT INFRINGEMENT IN AI TRAINING DATA

AI Training's Nature.
For training, generative AI systems need massive amounts of data. This information comprises: Books, Pictures, Videos, Music, Code, The posts on social media, Scholarly publications.
Web scraping techniques are widely used by AI engineers to gather publically accessible content from the internet. A large portion of this content is covered by copyright laws.
Copying works into datasets, transforming them into machine-readable representations, and identifying patterns within them are all steps in the training process.
Why Copyright Problems Occur.
Creators are granted exclusive rights under copyright law to make copies of works, distribute the work, get derivative works ready, publicly exhibit artwork.
Because copyrighted works are duplicated during dataset creation and processing, AI training frequently involves the reproduction right. Rights holders contend that the commercial exploitation of creative labour by AI businesses is profitable.

The Problem of Reproduction:
Copyrighted resources must be stored and analysed in order to train generative AI. Because digital copies are made, even if only momentarily, scholars contend that this technique can be considered reproduction under copyright law. AI firms argue that instead of maintaining emotive content, machine learning only extracts statistical associations. Critics point out that contemporary generative models can occasionally produce outputs that are strikingly similar or replicate copyrighted content verbatim.

Over-fitting and Memorization.
"Memorization" or "over-fitting" is a significant issue. When AI systems replicate portions of training data too precisely, this happens.
For instance: Copyrighted picture reproduction, creating passages from books, copying musical compositions, replicating creative styles.
Because they imitate copyrighted expression rather than only learning abstract patterns, such outputs can constitute infringement.

AI developers have been the target of several lawsuits. AI systems were allegedly trained on copyrighted literature without permission, according to authors and publishers. Artists assert that their works and styles were imitated by image-generation systems. AI-generated summaries and reproductions, according to media corporations, compete with journalism marketplaces. Artificial intelligence-generated voice clones and synthetic songs that mimic artists are challenged by musicians. Future copyright jurisprudence will be greatly influenced by these cases.

2.2.1 OWNERSHIP AND AUTHORSHIP OF DEEP-FAKE GENERATED CONTEXT:

The Problem of AI Authorship

Authorship and ownership of AI-generated works are among the most contentious topics in contemporary IP law.
Conventional copyright frameworks presume that: The work is written by a human author, human intellectual exertion is reflected in creativity, authorship gives rise to ownership. These presumptions are called into question by deep-fake technologies, which allow AI systems to produce realistic media on their own with little assistance from humans.
Principles copyright is mainly Human-Centric i.e. only human authors are recognized by the majority of copyright laws in the world.

Who Is the Owner of Deep-fake Content?

A number of potential claimants could claim ownership of deep-fakes produced by AI:
The developer of AI, the user asking the AI, the training data owner, the person portrayed, nobody (public domain). Different ethical and legal questions are brought up by each strategy.

AI Developers' Ownership.

AI firms may assert ownership due to:

The program was developed by them, the model was trained, the developers made resource investments. Ownership of software does not, however, always translate into ownership of all AI-generated output.

User Ownership

Some contend that since they direct the creative process, users who offer cues and instructions ought to be the owners of the results. This method is similar to ownership concepts in digital design or photography, where tools support human creativity. Determining an adequate human contribution is still challenging, though.

Theory of Public Domains:

According to a different theory, since there is no human creator, works created entirely by AI should stay in the public domain. Although this strategy encourages public access, it might deter investment in creative AI.

Ownership Conflicts and Personality Rights:

Real people are frequently portrayed in deep-fakes. Copyright ownership and personality rights clash as a result.

For instance: A user produces a fake actor's video.

The video produced by AI might use unique language.

Nevertheless, the actor's image is used without permission.

Personality rights may limit the resulting work's commercial use even if copyright is present.

Authorship Guidelines.

The degree of human involvement in AI-assisted projects is being assessed by courts more and more. Among the pertinent factors are:

Inventive rapid choosing.

Modification and editing.

Organizing outputs by hand.

AI autonomy level.

Copyright protection is more likely if human ingenuity predominates.

Issues with Joint Authorship

AI-related complex projects may require several contributors:

Creators of datasets, Programmers, Quick engineers, Editors, Final consumers etc.

When contributions overlap, it becomes challenging to determine shared authorship.

AI and Moral Rights

Moral rights concepts are complicated by AI-generated works because attribution could become ambiguous, without permission, artists' styles may be imitated, reputations may be distorted by deep-fakes.

Artists are calling for more control and acknowledgment when their creative identities are imitated by AI.

Economic Consequences:

Large companies may control the creative industries through automated content creation if AI-generated works are granted copyright protection.

Denying protection, on the other hand, might lessen the motivation for AI innovation.

For policymakers, striking a balance between these interests continues to be a major task.

The New Developments needed in Law

Courts and governments are looking on potential reforms like:

AI-generated content must be disclosed, watermarking digitally, copyright regulations unique to AI, licensing regimes based on consent, acknowledgment of rights to synthetic identities.

But as of right now, there is no universal legal framework.

2.2.2 THE DOCTRINE OF "FAIR USE" vs. UNAUTHORIZED DIGITAL CLONING

What Fair Use Means:

The legal concept of fair use is mainly accepted in the US. Under specific circumstances, it allows limited unapproved use of copyrighted content. The doctrine aims to strike a balance in Creators' protection, the right to free speech, creativity, the interest of the public.

The Four Fair Use Factors.

i. **Goal and Type of Use**

The Courts consider if the usage is non-commercial or commercial, reproductive or transformative. Fair use is more likely to apply to transformative uses.

ii. **Character of the Copyrighted Content**

Factual works are not as strongly protected as creative ones.

iii. **Quantity and Significance**

Courts evaluate the extent to which the original work was utilized.

iv. **The Impact on the Market**

This aspect looks at whether the use hurts the original work's market value.

Fair Use and AI Training

Model training, according to AI businesses, is fair use because it creates statistical representations from data, results are not the same as the original works, the training is similar to indexing or search engine operations.

Criticism of Claims of Fair Use

Opponents contend that AI systems are essentially different from human learning due to the following:-

Large-scale replication, exploitation for profit, automated duplication, substitution in the market. Publishers and artists argue that generative AI poses a threat to creative labour markets.

Unauthorized Digital Cloning

The term "digital cloning" describes the unapproved duplication of an individual's speech, the face, appearance, motions, also the creative identity.

Such cloning is becoming more and more affordable because of the deep-fake technology. Examples consist of:

Artificial celebrity endorsements, songs produced by AI that imitate musicians, the digital resuscitation of actors who have passed away.

The Problems with Digital Cloning

Digital cloning without authorization may violate copyright legislation, trademark legislation, rights of personality, rights to privacy, the law against defamation.

Victims could be harmed by financial losses, damage to one's reputation, emotional anguish and the exploitation of identity.

The Conflict in Between Fair Use and Digital Cloning:

Whether AI-generated imitations are criminal appropriation or transformative expression is the main legal dispute.

Justifications for Fair Use Advocates contend that new forms of expression are produced by AI, copyright does not apply to artistic styles, widespread access to training data is necessary for innovation.

Excessive limitations could impede scientific research and technological advancement, according to some academics.

Arguments Opposed to Fair Use

Critics contend that deep-fakes directly take use of people's identities, human performers are replaced by voice cloning, AI outputs and originals are in commercial competition, unauthorized cloning compromises consent.
They argue that the exploitation of a person's identity or creative effort should not be justified by fair usage.

Economic Substitution and Market Damage

Market substitution is one of the most compelling arguments against fair usage. For instance AI-generated graphics could take the place of human artists, voice actors may be replaced by synthetic voiceovers, and the deep-fake actors could make it harder to find work. The Courts may reject fair use claims if AI-generated content directly competes with original works.

Moral Aspects

The fair use controversy touches on ethical in addition to legalities.
Among the crucial ethical issues are, Should AI training be paid for by creators?
Is it possible to innovate without consent?
Should the digital rights of the deceased be preserved?
Is it possible to market human identity indefinitely?

These problems draw attention to conflicts between human dignity and technical advancement.
Balanced Regulation Is Necessary
More and more experts support fair regulatory regimes that safeguard artists and people, promote creativity, encourage openness, assure responsibility and avoid abuse.

CHAPTER 3
SOCIAL IMPACT OF DEEP-FAKES ALONG WITH THE REGULATORY APPROACHES FOR DEEP-FAKE AND INTERMEDIARIES:

3.1 Social impact of deep-fakes:

The digital ecosystem has entered an era of "synthetic media," where music, video, text, and images may be artificially created, thanks to the quick development of artificial intelligence (AI), machine learning, and generative adversarial networks (GANs).

Incredibly realistically altered. "Deep-fakes," a word used to depict hyper-realistic manipulated media produced using deep learning algorithms, are among the most contentious examples of synthetic media. Deep-fakes can mimic voices, gestures, facial expressions, and even emotions, making it difficult to distinguish between reality and application. However, they have rapidly developed into a tool that can affect public opinion, violate privacy, interfere with democratic processes, and violate intellectual property rights. Concerns about false information, non-consensual pornography, identity theft, defamation, and copyright breaches have grown as generative AI technologies become more widely available.

Deep-fakes provide a complex legal problem from the standpoint of cyber law. The intricacies of synthetic media were not intended to be addressed by the legal frameworks that were in place in India and around the world. Conventional beliefs on copyright, privacy, AI-generated works and digitally cloned identities are difficult for authorship and personality rights to accept.
Concern regarding deep-fake harms has grown among Indian judges and academics, particularly in cases involving public figures, political disinformation, and AI-generated likeness exploitation. Recent court cases in India show how personality rights and privacy risks related to synthetic media are becoming more widely acknowledged.

3.1.1 Effects on Democratic Conversation and Truth

The decline in public confidence in visual evidence is one of the most hazardous social repercussions of deep-fakes. In the past, photos and movies were trustworthy sources of evidence. This trust in evidence is compromised by deep-fakes.

The rise of "liar's dividend" has grown to be a serious issue. This idea describes circumstances in which people reject authentic evidence as fraudulent in order to avoid responsibility. Politicians who are accused of wrongdoing may argue that real videos are manipulated by artificial intelligence.

Additionally, deep-fakes have been used as weapons in elections to distribute false information, trick voters, incite conflict within the community, it can tarnish the political reputations.
The democratic atmosphere in India is especially precarious because of the high usage of social media, quick spread of false information, diversity in language, low levels of digital literacy.

Social and Psychological Damage
Deep-fakes are digitally produced or altered photos, videos, or audio recordings that give the impression that someone is saying or doing something that never happened. Deep-fakes are now simpler to produce and disseminate due to the quick development of artificial intelligence and social media. Many deep-fakes are made with malicious intent, even though some are intended for amusement or instruction. Because deep-fakes target a person's identity, dignity, reputation, and mental health, the social and psychological harm they do is exceedingly severe. As the falsified content spreads online, victims frequently endure silent suffering. Deep-fakes have an effect on more than just individuals; they can erode public confidence in online information and digital communication.

Emotional anguish is among the most detrimental consequences of deep-fakes. When victims come across phony content online that uses their voice or face, they frequently feel violated, horrified, and powerless. It can be quite painful to see oneself misrepresented in inappropriate or humiliating circumstances. Because it feels like they have lost control over who they are, many victims report the experience as extremely upsetting. When the content quickly spreads across other social media platforms, the psychological strain gets even worse. Victims may always worry about who has viewed the material and how others may perceive them.

Another significant effect of deep-fakes is social humiliation. False photographs or videos can harm a person's reputation among friends, family, co-workers, classmates, and the broader public. People may continue to question the victim's innocence even after the content is shown to be fraudulent. Sensational content frequently elicits fast reactions from society without fact-checking. Victims may thus become the focus of the gossip, mockery, and public humiliation. Some people avoid social situations out of fear of being ridiculed or evaluated by others.

Deep-fakes can potentially wreak significant damage to a person's reputation. With an edited video might falsely depict someone participating in unlawful, immoral, or unethical activities. This can undermine the value of hard labour, trust, and professional achievement in a relatively short period of time. Public figures, professionals, and teachers. Both business executives and ordinary citizens might become victims. When a person's internet reputation is tarnished, it is incredibly difficult to regain trust. Search engines and social media platforms may continue to display the bogus content long after it has appeared, creating long-term reputational damage.
Depression and anxiety are common psychological consequences reported by deep-fake victims. Constant stress, fear, embarrassment, and public pressure can have a bad impact on mental health. Victims may feel powerless because they cannot completely prevent the spread of fraudulent content. Anxiety is frequently caused by fear of social criticism, professional harm, or risks to one's personal safety. In severe circumstances, sufferers may experience insomnia, panic attacks, a lack of confidence, and emotional isolation. Some people may need professional counselling or treatment to heal from the psychological trauma induced by deep-fakes.

Deep-fakes can also result in job losses and career setbacks. Following the discovery of distorted content online, the employers may question a victim's character or credibility. Employees may face suspension, termination, or missed career chances as a result of false charges made using deep-fakes technology. Business professionals may lose clientele, relationships, or public trust. Students and job seekers may also suffer when fraudulent videos harm their academic or professional reputations. Even if the content is later revealed to be fraudulent, considerable damage may have already been done.

The viral nature of digital platforms exacerbates the matter significantly. Social media allows content to be shared internationally in minutes. Once a deep-fake has been shared, downloaded, reposted, or replicated across several platforms, it is very impossible to remove completely.

Even if the original source is destroyed, other versions may still circulate online. This permanent digital presence causes ongoing concern for victims since they are aware that the content may return at any time. The rapidity of online sharing also increases the scope of harm before fact-checking or legal action is taken.

Deep-fakes are highly associated with cyberbullying. Individuals, particularly teenagers and young adults, may become targets of online harassment via manipulated media. Bullies utilize phony recordings and images to humiliate, threaten, or socially isolate people. Deep-fakes, which appear genuine, can easily mislead viewers and amplify online abuse. Victims of cyberbullying frequently experience fear, loneliness, and emotional distress. Continuous online attacks can harm academic achievement, social relationships, and self-esteem.

Another risky application of deep-fake technology is vengeance pornography. In numerous circumstances, an individual's face is digitally substituted into sexual or indecent content without their permission. Women are disproportionately affected by such abuse. These false sexual recordings are frequently used to humiliate, dominate, or punish individuals following personal disagreements or relationship breakdowns. Revenge pornography violates privacy, dignity, and personal rights. Victims may suffer considerable emotional suffering. Social shame. And long-term psychological distress. The threat of such exploitation fosters insecurity and distrust in online communities.

Deep-fakes are increasingly being used in blackmail and extortion. Criminals may fabricate films or audio recordings to intimidate victims and extract money, personal information, or other favours. Victims may fear that others will accept the phony content, causing them to remain silent or comply. In certain cases, scammers employ deep-fake voice technology to imitate family members, business executives, or government officials. Such crimes can result in financial loss, mental distress, and serious legal consequences.

Beyond individual pain, deep-fakes cause larger social problems. One of the most serious risks is a loss of faith in digital communication. As deep-fakes get more lifelike, consumers may begin to question the veracity of genuine movies, pictures, and audio recordings. This causes misunderstanding regarding what is true and false. False information can quickly spread, swaying public opinion and undermining societal harmony. Deep-fakes could potentially be used to convey political propaganda, sway elections, or incite social unrest.

The erosion in faith in the media has an impact on journalism and law enforcement. Education and public communication. People can allege that real recordings are false, which calls authentic evidence into question. Dishonest people refute genuine facts by blaming deep-fake technology, a situation known as the "liar's dividend." As a result, society may struggle to separate reality from manipulation. This reduces trust in internet information and undermines democratic discourse.

Deep-fakes induce psychological terror, which influences how individuals behave online. Individuals may become more careful while sharing images, videos, or personal information on social media. Some people may avoid participating in digital areas entirely because they fear the misuse of their identity. This limits freedom of expression and causes anxiety during online conversations. Trust between individuals may erode because people no longer feel convinced about the authenticity of digital content.

Children and teenagers are especially sensitive to the negative consequences of deep-fakes. Young individuals may not completely comprehend how manipulated media works, making them easy targets or inadvertently spreading misleading

information. Exposure to humiliating or explicit deep-fakes can have major consequences on emotional development and mental health. Schools and parents thus have an essential role in educating children about digital safety, ethical internet use, and media literacy.

Governments, tech businesses, and educators and society must work together to mitigate the negative effects of deep-fakes. Strong laws and regulations are required to penalize individuals who perpetrate malicious deep-fakes. Social media platforms should enhance their mechanisms for recognizing and removing manipulated information rapidly. Artificial intelligence systems can also aid in detecting bogus media before it spreads widely. Public awareness initiatives are necessary to teach individuals how to verify information and prevent distributing erroneous content.

3.1.2 ECONOMIC AND CYBER SECURITY CONCERNS

Deep-fake voice cloning has emerged as a major economic and cyber security issue as it is being used in sophisticated fraudulent activities. Cyber criminals can now create incredibly realistic synthetic voices that resemble executives, public personalities, and even family members with startling precision. These technologies have been used in financial fraud, business impersonation, CEO scams, and phishing attacks, in which attackers trick victims into sending money, giving sensitive information, or granting illegal access to confidential systems. For example, fraudsters may utilize cloned voices to mimic senior company officials and tell employees to do urgent financial transactions, taking advantage of confidence and authority within organizations.

Furthermore, the proliferation of synthetic identities has raised worries about the trustworthiness of digital identification methods. Many enterprises increasingly rely on voice recognition and biometric verification for security; however, deep-fake technologies weaken these processes by successfully duplicating an individual's vocal features, allowing them to evade authentication protocols. As a result, cyber security infrastructures are increasingly vulnerable to identity theft, unauthorized system access, and large-scale social engineering attacks. As a result, deep-fake voice cloning is not only a scientific problem, but also a significant threat to economic stability, organizational trust, and digital security in modern society.

3.1.3 IMPACT ON WOMEN AND ON THE MARGINALIZED COMMUNITIES

The advent of deep-fake technology has raised severe ethical, social, and psychological concerns, especially among women and underprivileged groups. Deep-fakes are digitally altered photos, movies, or audio recordings made with artificial intelligence to impersonate genuine people. While technology can be utilized to entertain, educate, and innovate, its misuse has disproportionately hurt society's most vulnerable people. The impact goes beyond individual victims to address greater issues of gender inequality, discrimination, and misuse of power in digital environments.

Women are among the most common victims of malevolent deep-fake content, particularly non-consensual deep-fake pornography. According to research, women account for the vast majority of deep-fake pornographic material available online, including celebrities, journalists, politicians, and everyday people. In many situations, women's faces are digitally overlaid on sexual content without their knowledge or permission. This type of exploitation undermines privacy, dignity, and physical autonomy.

Victims face harsh and multifaceted consequences. Women subjected to deep-fake pornography frequently experience emotional pain, embarrassment, anxiety, despair, and reputational harm. Such content can harm personal relationships, careers, and social standing. In professional settings, women may lose trust or endure harassment as a result of edited content that incorrectly shows them in vulnerable situations.

Furthermore, deep-fake abuse mirrors and perpetuates patriarchal frameworks that have traditionally objectified and controlled women's bodies. Technology becomes yet another tool for perpetrating gender-based violence in the digital realm. Because women already suffer greater rates of online harassment and cyber abuse, deep-fakes exacerbate existing inequities rather than introducing wholly new kinds of discrimination.

Now, for marginalized group the impact are as follows:

Hate propaganda

Deep-fakes can be used to disseminate hate against marginalized groups by fabricating films or statements that promote stereotypes, provoke violence, or support prejudice. Manipulated media may depict members of minority communities as engaging in criminal, immoral, or anti-national acts. Such information can exacerbate prejudice, social antagonism, and communal problems.

The quick spread of misinformation via social media platforms exacerbates the danger. Many viewers may fail to recognize edited content, reinforcing harmful biases and hostility toward already vulnerable communities.

Targeted misinformation

Marginalized groups are likewise vulnerable to targeted misinformation efforts designed to influence public opinion or suppress political involvement. Deep-fakes can be strategically used to undermine activists, community leaders, or social movements by portraying them as dishonest, violent, or radical. During elections or political confrontations, misinformation can undermine democratic participation and marginalize minority views.

Targeted misinformation is especially destructive since underrepresented communities may already have limited access to accurate media coverage. Deep-fake technology thus heightens the likelihood of social exclusion and political marginalisation.

3.1.4 Cultural Manipulation

Deep-fake technology can also help to manipulate cultural narratives by distorting minority communities' identities, traditions, and histories. Artificially generated content may distort cultural practices, religious beliefs, or historical events, resulting in confusion and cultural erasure. In certain circumstances, deep-fakes are used to mock or criticize cultural identities for amusement or political purposes.

This manipulation jeopardizes the legitimacy and integrity of cultural representation in digital environments. For populations already striving for recognition and equality, such misuse of technology exacerbates social estrangement and hinders attempts to promote inclusion and respect.

3.1.5 Reinforcement of social inequalities

One of the most troubling elements of harmful deep-fakes is how they exacerbate existing societal inequities. Technology is typically viewed as neutral; nonetheless, its implementation reflects societal biases and power systems. Deep-fake abuse disproportionately impacts populations who already face discrimination, harassment, and little protection from social and legal systems.

Deep-fakes maintain patriarchal domination by transforming women's identities into targets of exploitation and humiliation. For oppressed groups, technology becomes a tool for disseminating hatred, ignorance, and cultural distortion. As a result, deep-fakes do more than only cause new digital problems; they exacerbate long-standing inequities based on gender, ethnicity, class, sexuality, and political power.

3.1.6 Threat to media and journalism

Synthetic media, particularly AI-generated content such as deep-fakes, altered audio, forged articles, and manipulated videos, pose a significant threat to journalism and public trust. Because this content can closely resemble genuine persons, events, and news reports, it is difficult for viewers to distinguish between truth and deception.

- Synthetic media harms journalism by presenting fake content as legitimate.

Journalism relies on accuracy, proof, and public trust. Synthetic media weakens these underpinnings by making bogus information appear incredibly realistic. All systems can generate films, audio, photos, and written reports that simulate genuine events or individuals. For instance, a bogus video could show a government leader spreading misleading information.

Edited audio clips may imitate journalists or celebrities, while AI-generated articles may mimic reputable news organizations' style.
Many individuals receive news quickly through social media, so they may believe and distribute erroneous information before it is validated. This harms the reputation of legitimate journalism by leading audiences to question whether any content is genuine.
Another risk is that genuine reporting is misinterpreted as fraudulent. This phenomenon, known as the "liar's dividend," occurs when those accused of crime dismiss real evidence by claiming it was manufactured by artificial intelligence.

- Deep-fake news reports are falsified broadcasts or videos made using artificial intelligence to mimic real news outlets, reporters, or events.
How they function Al can:
IT can replicate a person's face and voice, it can also recreate the newsroom settings, create realistic video footage, can create credible news scripts.
Deep-fake reports are dangerous because they appear professional and trustworthy, leading to the rapid spread of misinformation. Viewers may not recognize tampering, especially if the logos, presenters, and visuals mimic those from reputable news networks.
Possible effects are as follows:
Can provide false political information during elections, fake emergency announcements, manipulated financial news, which impacts the markets, can do harm to the reputations of prominent figures or organizations.

- Interviews were fabricated.
Fabricated interviews include fabricating fictitious discussions or remarks that never occurred.
Methods which Al tools can use are as follows:
They can create realistic voices, can record lip-synced video footage, it can create fully imaginary dialogue. A public figure may appear to be offensive and provocative or deceptive remarks, even if they never made them.
The consequences are as follows:
It Damages to the personal and professional reputations of the individual, it can help in spreading political propaganda, also can help in the manipulation of public emotions, it can cause loss of confidence during genuine interviews. Journalists may also have difficulties in confirming the authenticity of genuine recordings once false copies become ubiquitous.
Also it can generate manipulated war film which can cause misunderstanding during emergencies, during wartime, natural disasters, or emergencies, people depend greatly on media for accurate information. Manipulated footage might alter reality during these sensitive times.
Examples of AI-generated videos are it can show the attacks that never happened, it can also make exaggerated claims about devastation or casualties, it can misrepresent military operations, this may also spread phony humanitarian emergencies.
This particularly harmful in various crisis situations like:
Whenever people see something related to crisis, they respond emotionally and fast, also the governments and corporations make critical decisions during such situation, panic spreads quickly by such misinformation.
False film can amplify fear and incite violence. It could cause diplomatic problems between nations. It may also disrupt rescue operations or humanitarian relief activities.
P.T.O

3.2Analysis of domestic frameworks

A. DPDP ACT

So, first of all we will study the newly enacted DPDP Act 2023, in this act it had made compulsory to give the consent for the data which is acquired by the data fiduciary from the one who is generating the data, the data collected must be for a specific purpose, unconditional and free from any kind of ambiguity. Here, the compulsory unconditional consent had made the data of the users vulnerable for the cyber-crimes. The users are not getting the chance for giving their consent according

their own will. It is called as the Rights of Data Principal. One of the most famous case, which was happened recently before the act came into force is as follows:

It was made against the policy of sharing the users data is Facebook India Online case, here in this case, the data of the Whatsapp users were shared with the Facebook and if the Whatsapp will not share the data with Facebook, it will lead to the termination of the services. In this case, the honorable Delhi High Court held that this sharing of data is unreasonable and is not fair for the users of Whatsapp. But, in spite of this the policies for the protection of the data, in scenarios like this is not being discouraged by the DPDP Act, and thus, the data shared can be used for various purposes including for AI training also, as the data shared are with the consent of the users only.

B. INFORMATION TECHNOLOGY ACT, 2000.

In India, the act dealing with cyber-crimes is no other than IT Act 2000. The act was influenced by the UNCITRAL Model Law on E-commerce also, the IT Act was amended in the year 2008 due to the emerging cyber-crime threats. But at the time of enactment of the IT Act, it was considered progressive and a kind of ahead of time. There are a lot of cyber related offences which are recognized under the IT Act 2000. They are given under chapter 11 “OFFENCES”. This act covers various kinds of cyber-crimes like, the offence of tampering with the computer related documents, offences related to computer, transmitting obscene material with the help of electronic medium of data transfer.

Now, as we can see that the act came in the year 2000, and at that time AI was not there, as it came before the evolution of AI, machine learning and deep-fake technologies, it lacks in provisions regarding the crimes committed with the help of these new technologies.

The deep-fake cases has an indirect intersection with various crimes like defamation, identity theft, privacy violations, financial scams, sexual harassment etc.

But, in the IT Act the word deep-fake is no-where mentioned. Still it deals with the cases of deep-fakes to a certain extent by the help of various other provisions which are somewhere, indirectly linked with the deep-fake crime. Few examples of these kind of sections are as follows:

v. Identity Theft [section 66C]: It stipulates that anyone who fraudulently or dishonestly uses another person's electronic signature, password, or other distinctive identifying feature faces a maximum sentence of three years in prison and a fine of up to one lakh rupees.
However, it is also unclear if voice cloning and face identity fall under the definition of unique identification.

vi. Violation of Privacy [section 66E]: This provision states that anyone who publishes or transmits someone else's private photos without that person's permission is violating that person's right to privacy.
The majority of the time, this part is utilized while dealing with altered private photos and videos.
However, it is not made clear in this provision that images or films created with artificial intelligence will fall under its purview.

vii. Transmitting Obscene material in electronic form [section 67 and 67A]: Are mainly used in the cases related to deep-fake pornography.

viii. Controlling Power of the government [section69A]: It authorizes the government that if they think that any content might hamper the sovereignty, national security, public order of a country.

C. THE INTELLECTUAL PROPERTY LAWS

In the Intellectual property laws, there is a concern regarding the authorship of a AI generated content. The acts like the copyright act was made according to the human creativity but today the contents are now being generated by the AI, thus there arises a question regarding the authorship and ownership of the content. The definition of author given under the

copyright act is not taking about the AI. So, the programmer, the developer of the platform using AI deep-fake content, the user etc. who is said to be the owner of the content.

Also, there is a concern of copyright infringement happening on the name of training data. Many data which are given to the AI are not given by the consent of the user, they are mostly collected from the online sources without the consent of the user.

D. CONSTITUTION LAW

There are certain articles under the constitution of India, which are majorly being affected by the deep-fake. Especially the right to freedom of speech and expression along with right to privacy are majorly being affected by the deep-fakes. Here, in right to freedom of speech and expression the major challenge is to maintain a balance between speech freedom and it's protection against the digital harm. Like article 19[1][a] protects freedom of speech but does it applies the same way when memes are created with the help of deep-fake and are further being transmitted.

The constitution doesn't clearly talks about right to personality like name, face, voice under the ambit of right to privacy, but the judiciary have gradually recognized it. But, then comes the deep-fake which mostly replicate the individual's replica without his/her consent.

E. The newly introduced criminal code [BNS,2023]

India just replaced the colonial-era Indian Penal Code of 1860 with the "Bharatiya Nyaya Sanhita" of 2023 (BNS). The BNS went into effect on July 1, 2024, and aims to modernize Indian criminal law by identifying cyber-enabled offences and the technology based crimes. However, the legislation lacks a precise provision for defining or criminalizing deep-fakes. Instead, deep-fake related wrongdoing is dealt indirectly through regulations dealing with forgery, defamation, disinformation, obscenity, cheating, impersonation, organized crime, and public order violations.

The BNS's legal treatment of deep-fakes demonstrates both progress and severe legislative deficiencies. The legislation tries to apply ancient criminal theories to current technological harms, but the lack of exact statutory language generates interpretive confusion and enforcement issues.

Understanding Deep-fakes in Legal Context

Deep-fakes use artificial intelligence algorithms, particularly deep learning models, to create synthetic material that appears legitimate. These modified files may include face-swapping movies, AI-generated voices, morphed photographs, fabricated speeches, fraudulent corporate communications, and misleading social media posts.

The legal issue arises because deep-fakes can be used for a variety of illicit activities. They can harm reputations, incite communal hatred, rig elections, encourage cyber fraud, or sexually exploit individuals. In India, women are more vulnerable to nonconsensual deep-fake pornography.

The difficulty for criminal law is assessing whether existing charges are broad enough to encompass AI-generated synthetic media. Because deep-fakes are not always "false documents" in the usual sense, courts must construe customary prohibitions broadly to incorporate digital manipulations.

The Indian government has explicitly stated that AI-generated harms, such as deep-fakes, are actionable under existing laws. The Press Information Bureau has suggested that sections of the BNS, the Information Technology Act of 2000, and related guidelines can be used to combat deep-fake usage.

But, many of the legal scholars have noted that the BNS is generally technologically neutral, with no explicit definitions of synthetic media or deep-fake crimes.

Below are some of the sections Of BNS, which indirectly deals with Deep-fakes.

i.Defamation under Section 356One of the most important rules related to deep-fakes is Section 356 of the BNS, which criminalizes defamation. Deep-fakes frequently depict people committing acts they did not commit, so undermining their reputation and dignity.

For example: A manufactured film depicting a public figure making offensive statements, morphed intimate content concerning a private individual, or an AI-generated content falsely identifying a person with criminal behavior.

Such activity directly harms reputation and may result in criminal charges under defamation legislation. Legal analysts acknowledge that modified or synthetic media can be "visible representations" capable of defaming individuals.

From a legal sense, the application of defamation law to deep-fakes illustrates a link between established criminal doctrines and contemporary technologies. The substance of the violation is reputational harm, regardless of the technology means used.

ii.Forgery and Fabrication of Electronic Records:

The BNS classifies electronic records as forgery offences. Section 337 specifically tackles the falsification of electronic records and government-issued papers. Although deep-fakes are not explicitly addressed, AI-generated material may be classified as fabricated electronic records if they are made with the aim to deceive or harm. For example: An adulterated government announcement video, a fabricated courtroom recording, identity documents manufactured by artificial intelligence, or manipulated biometric data.

The introduction of "electronic records" is significant since it updates traditional forging principles for the digital age. However, conceptual confusion continues because deep-fakes do not always require the modification of an existing document. Some are wholly synthetic, derived from datasets.

iii. Cheating and Personification

Deep-fakes are increasingly being utilized for financial crime and impersonation. AI-generated voices can impersonate CEOs, relatives, or government officials to trick victims into moving money or exposing sensitive information. In such instances, the BNS regulations governing cheating, dishonest inducement, and impersonation may apply. The deceptive use of synthetic media to obtain property or inspire reliance meets the key elements of cheating offenses.

The illegality is not just in creating fraudulent information, but also in employing deception to obtain wrongful benefit or create wrongful loss.

iv. Public Mischief and False Information [Section 353]

The government has emphasized that Section 353 of the BNS can be utilized to combat misinformation and misleading news distributed by deep-fake technology.

Deep-fake videos may be used to promote communal violence, create panic during emergencies, manipulate elections, reduce public trust in institutions, or to cause social turmoil.

Section 353 punishes false or deceptive remarks that are likely to cause fear, panic, or public unrest. This feature is especially relevant in circumstances of political deep-fakes and disinformation campaigns. The rise of AI-generated propaganda creates constitutional issues such as democratic integrity and electoral fairness. Deep-fakes blur the distinction between truth and fiction, hurting informed public debate.

v. Organized Crime under Section 111 of BNS.

Under Section 111, the BNS creates a new organized crime offence. Legal experts have stated that large-scale coordinated deep-fake operations may be covered by this section if synthetic media is utilized routinely for crimes or financial fraud. For example, organized extortion using altered intimate videos, coordinated election manipulation efforts, Al-enabled financial scams etc. This section recognizes that cybercrimes are becoming more networked and global. However, Section 111's broad scope has drawn criticism for its ambiguity and potential for abuse.

vi. Obscenity and Sexual Exploitation

Deep-fake pornography is one of the most dangerous kind of Al abuse. Women, celebrities, journalists, and students have all been targeted with nonconsensual intimate deep-fakes. Although the BNS does not directly specify AI-generated sexual content, regulations pertaining to obscenity, voyeurism, insult to modesty, and sexual harassment may be used. In addition, the Information Technology Act expands criminal culpability in cases involving the transmission of obscene electronic data.

From a feminist legal perspective, deep-fake pornography violates:

Bodily autonomy, sexual Dignity and privacy.

Victims frequently experience psychological implications such as trauma, reputational damage, social isolation, and professional injury.

3.3 International perspectives:

Deep-fakes affect privacy, democracy, cyber-security, human rights, and public trust across national boundaries, therefore the international viewpoint on them is vast and growing. Instead of a single global legislation, different countries and international organizations are tackling the issue through a variety of legal and policy frameworks.

a) Data protection laws

Many countries have regulations in place to protect and regulate deep-fakes. Deep-fakes frequently use a person's picture, voice, or biometric data without permission. Regulations such as the European Union's AI and privacy frameworks prioritize personal data protection and mandate openness in the usage of AI-generated material. These regulations are intended to prevent identity fraud and unlawful manipulation of personal information.

b) Laws Concerning Cyber-security Because deep-fakes can be exploited for fraud, identity theft, disinformation campaigns, and social engineering attacks, they are becoming more and more recognized as cyber-security concerns. Deep-fake identification and prevention are being incorporated into national cyber-security policies by a number of countries. International organizations acknowledge that false information produced by AI has the potential to erode digital security and trust.

c) Laws Concerning Election Integrity Deep-fakes have the potential to sway public opinion, disseminate false political information, and tamper with elections, which worries many democracies. As a result, nations are creating legislation requiring the labeling or disclosure of political content produced by AI. To lessen the possibility of misleading synthetic media influencing political processes, the European Union, for instance, established transparency obligations under the Al Act.

d) Privacy Laws

In order to mitigate the negative effects of non-consensual deep-fakes, particularly those including intimate or libelous content, privacy frameworks are employed. Victims may experience mental suffering, harm to their reputation, and abuses of their dignity. Unauthorized production and dissemination of such content is considered a violation of personal autonomy and privacy rights in many jurisdictions.

e) Frameworks for Intellectual Property
Because Al systems may mimic copyrighted materials, voices, performances, or likenesses, deep-fakes can pose a threat to intellectual property. Countries are investigating whether regulations pertaining to copyright, trademarks, and publicity rights can safeguard artists and celebrities. Protecting popular figures from commercial exploitation and unapproved digital duplication.
f) Provisions of Criminal Law For detrimental uses of deep-fakes, such as fraud, harassment, revenge pornography, child abuse, or electoral meddling, some nations have imposed criminal penalties. Malicious production and dissemination of misleading synthetic media are increasingly being penalized by criminal law.
g) Standards for Human Rights International organizations emphasize that responses to deep-fakes must strike a balance between security, freedom of expression, and other human rights. UNESCO and the OECD, for example, support human-centered Al governance that upholds democratic values, privacy, and dignity while promoting responsible innovation.
h) The necessity of international cooperation due to the rapid cross-border dissemination of deep-fakes via social media and online platforms, national regulations are no longer enough. Therefore, information exchange, uniform laws, technical standards, and enforcement procedures all depend on international cooperation. To effectively counteract cross-border misuse of deep-fakes, international organizations are promoting cooperation or Al transparency, watermarking systems, detecting technology, and ethical Al governance.

3.3.1 Deep-fakes And International human rights law:

Deep-fake have emerged as a major global concern because they have the potential to seriously undermine fundamental human rights. International human rights law protects privacy, freedom of expression, dignity, and reputation. However, the misuse of artificial intelligence via deep-fake technology poses significant egalitarian and ethical issues to governments and international organizations.

a. Right to Privacy.

International human rights law protects the right to privacy as follows:

Article 12 of the Universal Declaration of Human Rights,

Article 17 of the International Covenant on Civil and Political Rights.

These provisions declare that no one shall be subjected to unlawful interference with their privacy, family, home, or reputation. Deep-fake technology can infringe this right by using a person's face, voice, or identity without permission. It is extremely dangerous when people produce and disseminate phony intimate or graphic information online.

Women are frequently the major victims of non-consensual deep-fake pornography, which can cause embarrassment, emotional distress, harassment, and damage to personal dignity. Because these bogus documents can spread quickly via digital networks, victims may find it difficult to regain their privacy and social position.

International human rights law focus on the need to safeguard individuals from technological misuse that interferes with personal autonomy and dignity.

b. Freedom of expression.

It is recognized as follows:-

Article 19 of the Universal Declaration of Human Rights;

Article 19 of the International Covenant on Civil and Political Rights.

These provisions protect individuals' rights to express opinions, discuss ideas, and convey information through various types of media. Deep-fake technology is not always illegal because it can be utilized for entertainment, education, art, and political commentary.

However, difficulties arise when deep-fakes are used to disseminate false information, manipulate public opinion, instigate hatred, or disrupt democratic processes. Governments thus face a difficult task. On the one hand, they must prevent damaging falsehoods and safeguard society against deception.

On the other hand, severe regulation of deep-fakes may limit creativity, free speech, and lawful digital expression.

As a result, countries are trying to strike a balance between:

Technological innovation and free speech, individual privacy and human dignity, public security and democratic openness.

This balance remains one of the most contentious topics in international human rights law today.

c. Right to Reputation and Dignity

Deep-fakes can potentially seriously harm a person's reputation. Fake videos or audio recordings of politicians, celebrities, judges, corporate leaders, or ordinary residents may depict them as engaged in unlawful, immoral, or offensive behavior.

Such content may result in social isolation and public shame, loss of job or career opportunities, psychological trauma and emotional discomfort and political unrest and popular distrust.

International human rights concepts increasingly acknowledge that reputation is inextricably linked to human dignity. False and altered digital materials, even if later proven untrue, can have long-term consequences for how society perceives a person. Because deep-fakes can quickly propagate throughout social media sites, the harm caused is frequently immediate and impossible to rectify. This has prompted legal scholars and policymakers to call for better international collaboration and clearer laws controlling artificial intelligence and digital manipulation.

3.3.2 Approach of USA regarding deep-fake:

The United States' response to deep-fake is changing through a combination of federal laws, state restrictions, technology business rules, national security measures, and public awareness campaigns. The United States does not yet have a single comprehensive federal deep-fake law, but it does use a variety of legal and legislative mechanisms to mitigate the risks.

- Focus on harm rather than technology itself.

The United States' approach generally restricts the detrimental use of deep-fake rather than outright prohibiting Al-generated content. Policymakers understand that synthetic media can have valid purposes in entertainment, education, accessibility, and research. The government focuses on deep-fakes that involve election meddling, Fraud, impersonation, non-consensual explicit content, defamation and misinformation and national security threats. Federal agencies include federal trade commission, federal communications commission, and homeland security department, have warned that false Al material may violate consumer protection, cyber-security, and communication regulations.

- Election Protection Measures

One of the most stringent areas of regulation is elections. Several states in the United States have laws that prohibit fraudulent AI-generated political commercials near election time. These statutes typically requires labels indicating disclosure on AI-generated campaign content

Immediate removal of fraudulent electoral media, there are penalties for purposefully deceiving voters. The danger is that deep-fakes may represent candidates making deceptive comments or engaging in acts that never occurred.

- Criminalization of non-consensual Deep-fake pornography

Many states have implemented legislation prohibiting sexually explicit deep-fakes made without consent. These laws punish such content similarly to image-based sexual assault, or "revenge pornography". Victims may file criminal complaints, seek civil damages and can request content removal. Because of the significant psychological and reputational harm inflicted on victims, this issue has attracted bipartisan support.

- National Security and Cyber-security Concerns

U.S. security services see deep-fakes as a potential threat to military operations, diplomatic relations, public trust, financial systems etc.

Deep-fakes could be used for foreign disinformation campaigns, social engineering schemes, voice cloning fraud, identity impersonation.

The government, as a result, promotes research into Deep-fake detecting methods and also technologies for digital watermarking and media authentication.

- Cooperation with Technology Companies

The United States relies significantly on collaboration with private technology companies rather than direct regulation. Some of the major companies are Open Al, Google, Meta etc. Microsoft has implemented policies to label the AI-generated content and remove harmfully altered media, limits impersonation abuses, establish watermarking standards.

The U.S. government frequently supports voluntary compliance and industry norms rather than initiating severe centralized regulation.

- Protection of Free Speech

The American approach emphasizes the importance of balancing regulation with the constitutional right to free expression guaranteed by the First Amendment. Courts and lawmakers are concerned that overly broad deep-fake bans could restrict satire and parody, limit artistic expression, and interfere with political communication.

As a result, rather than outright prohibiting all synthetic media, US laws often focus on misleading intent, fraud, or quantifiable harm.

- Research and Technology Development

The United States government finances universities, defense agencies, and commercial laboratories to better development of Al detection tools, authentication verification systems, watermarking-technologies, media literacy programs. Organizations such as DARPA have funded research initiatives targeted at identifying altered audio and video.

- CHALLENGES:

Despite improvements, the United States continues to face various challenges like deep-fake technology develops rapidly thus detection tools are imperfect. Also, laws vary among states, cross-border online content is difficult to regulate, balancing innovation and regulation remains tricky.

3.3.3 UK

In order to create answers for new AI-related problems, the UK additionally promotes cooperation between academic institutions, research-center, businesses, and foreign partners. The nation aims to maintain its competitiveness in the global AI market while safeguarding public interests by promoting innovation in addition to regulation.

Challenges Faced by the United Kingdom are as follows:

The UK confronts a number of obstacles to successfully regulating deep-fakes despite continuous efforts. A significant challenge is striking a balance between the necessity to avoid dangerous content and the right to free speech. It is challenging to enact rules that target malevolent deep-fakes without restricting legitimate creativity because some modified media may-be-utilized-for-satire-and-creative-expression-or-amusement.
The speed at which technology is developing presents another difficulty. Detection systems frequently find it difficult to keep up with increasingly realistic AI-generated material, while deep-fake generating techniques continue to advance. Regulators and law enforcement organizations must therefore continuously modify their strategies.

Because deep-fake content can be produced in one nation and disseminated worldwide via internet platforms, cross-border enforcement presents additional challenges. Therefore, effective mitigation of digital harms requires-international-cooperation.

Concerns have also been raised regarding the possible abuse of AI detection systems. Automated moderation systems may make mistakes, misidentifying real content as fraudulent or failing to recognize complex manipulations. This emphasizes how crucial it is to combine technical solutions with legal protections and human monitoring.

Public Awareness and Digital Literacy

The UK acknowledges that the issues surrounding deep-fakes cannot be fully resolved by legislation alone. Digital knowledge and public awareness are equally crucial. People need to be able to assess online content critically and comprehend how manipulated media can affect people's beliefs and actions.
People are encouraged to check information before sharing it online via educational efforts and media literacy initiatives. Public institutions, educators, and journalists all contribute significantly to the dissemination of correct knowledge and the prevention of false information.

Initiatives that assist people in recognizing dubious digital information and comprehending the moral ramifications of AI technologies are supported by the government. Raising public awareness can enhance resistance to disinformation tactics and lessen the impact of dangerous deep-fakes.
Thus, we can say that in order to tackle the problems posed by deep-fakes and artificial intelligence technologies, the UK has taken a thorough and dynamic strategy. To successfully control digital hazards, the nation incorporates online safety legislation, data protection rules, criminal law reforms, cyber-security measures, and AI governance techniques rather than depending-on-a-single-legal-framework.

Digital platforms have significant obligations under the UK's Online Safety framework to keep an eye on and eliminate harmful information, including altered media. While criminal law improvements target malevolent actions like fraud, cybercrime, and intimate deep-fake abuse, data protection laws protect people from unlawful use of personal information. At the same time, the government prioritizes responsible AI development, cyber-security, and kid safety.

Even though there are still issues because of the speed at which technology is developing and the widespread use of digital communication, the UK is strengthening its laws and regulations. The nation hopes to establish a more secure and reliable digital environment by encouraging responsibility, openness, innovation, and public awareness. In the era of artificial intelligence, the UK's strategy highlights the significance of striking a balance between ethical responsibility, technological advancement, and the protection of individual rights.

3.3.4 The European Union Artificial Intelligence Act[EU AI Act]

The first comprehensive supranational law in the world that specifically regulates artificial intelligence systems is the European Union Artificial Intelligence Act (EU AI Act). The Act, which was formally passed as Regulation (EU) 2024/1689, creates uniform guidelines for the creation, application, commercialization, and use of AI throughout the European Union. Many people consider the bill to be a significant advancement in international regulatory policy, digital governance, technology law, and human rights regulation. The AI Act aims to strike a balance between innovation and the protection of democracy, the rule of law, public safety, basic rights, and consumer protection.
Rapid developments in machine learning, generative AI, biometric surveillance technologies, predictive systems, and automated decision-making gave rise to the AI Act. Concerns about algorithmic discrimination, opacity, manipulation, misinformation, privacy violations, labour displacement, and dangers to democratic governance were raised by the growing social and economic impact of AI systems. The General Data Protection Regulation (GDPR), consumer protection regulations, and product safety rules are examples of existing legal frameworks that were deemed inadequate to handle the

particular hazards presented by AI technologies. As a result, the EU implemented a risk-based regulatory structure designed especially for artificial intelligence.

The European Commission proposed a draft rule in April 2021, marking the start of the AI Act's legislative path. The final wording was approved in 2024 following protracted discussions between the European Parliament, the Council of the European Union, academia, industry players, and civil society organizations. Although many of the requirements will take effect gradually over a number of years, the regulation went into effect in 2024.

OBJECTIVES AND THE PURPOSE OF THE ACT

The AI Act's main goal is to enhance EU internal market performance while guaranteeing that AI systems uphold fundamental rights and European constitutional values. The Act's stated goal is to advance "human-centric and trustworthy AI," according to Article 1 of the Regulation. In order to allow enterprises to operate under a single legal framework and provide users with consistent protections, the law aims to establish uniform standards that apply to all Member States. Among the main objectives are as follows:

1. Ensuring AI systems are secure.
2. Preserving human dignity and fundamental rights.
3. Preventing manipulative or discriminating AI activities.
4. Improving responsibility and openness.
5. Encouraging investment and innovation in reliable AI.
6. Increasing the public confidence in AI systems.
7. Making Europe a global leader in the governance of ethical AI.

The European constitutional concept, which emphasizes proportionality, human autonomy, democratic accountability, and prudent governance, is also reflected in the AI Act. The EU approach takes a rights-based framework heavily inspired by the EU Charter of Fundamental Rights, in contrast to countries that promote innovation with less regulation.

SCOPE OF THE ACT

The AI Act has a wide range of material and territorial applications. It applies not only to organizations founded inside the EU but also to providers and the executor outside the EU if their AI systems have an impact on Union citizens. This extraterritorial application is similar to the worldwide scope of the GDPR.
The following are covered by the rule:
AI system providers entering the EU market. Also to the EU executors who use AI systems, AI system distributors and importers, product makers incorporating AI into their offerings. Suppliers of all-purpose AI models. The use of AI systems by private companies and public authorities.
However, some activities are not covered by the Act, such as:
AI systems that are only utilized for national security or military objectives. AI used only for personal or domestic purposes. Research and development activities in science under particular circumstances. Open-source AI systems in specific, constrained situations.

- **Artificial Intelligence Definition**

The definition of artificial intelligence was one of the most contentious topics during the drafting process. In order to prevent quick obsolescence, the final definition takes a technologically neutral stance. A machine-based system that can function with different degrees of autonomy and produce outputs like suggestions, forecasts, judgments, or content that affects real-world or virtual environments is referred to as an AI system under Article 3.

The EU's goal to make the law future-proof is reflected in the broad definition. However, some contend that a too broad scope could lead to legal ambiguity, particularly with relation to standard software systems and automated algorithms. According to scholarly criticism, ambiguous phrasing may cause problems with interpretation when it comes to court enforcement.

- AI Systems with Unacceptable Risk factor: Article 5 forbids some AI techniques because they are seen to be intrinsically incompatible with European values. These AI systems fall under the category of "unacceptable risk." Among the prohibited AI techniques are public authorities' social score systems, AI systems taking advantage of children's or people with disabilities' vulnerabilities, AI methods that are manipulative and harmful to the mind, Unintentional facial image harvesting from CCTV or the internet, Some systems of predictive policing, With a few specific exceptions, real-time remote biometric identification in public areas.

- These restrictions show how much the EU values democratic liberties, privacy, and human dignity. Concerns sparked in part by surveillance methods used in authoritarian governance systems are reflected in the ban on social scoring. In a similar vein, limitations on biometric surveillance aim to stop widespread monitoring and its detrimental impact on civil liberties.
However, several prohibitions have been critiqued by academics for being conceptually ambiguous. Judicial explanation may be necessary for terms like "exploitation," "manipulation," and "subliminal techniques."

- AI Systems which are at very high risk category: "High-risk" AI systems are subject to the AI Act's most specific requirements. These AI systems have the potential to drastically impact people's rights, opportunity, safety, or access to basic services. AI utilized in high-risk systems includes: Hiring, instruction and evaluation of students, banking and credit scoring, vital infrastructure, the police, border security and migration, medical equipment and administration of justice.
Now if, AI applied to assess job candidates, assess creditworthiness, or forecast criminal activity, for instance, may have a significant impact on basic rights. As a result, providers and executor of such systems are subject to stringent compliance requirements under the Act.

Requirements for AI Systems at High Risk

- Systems for Risk management: In order to identify predictable risks related to the implementation of AI, providers must set up ongoing risk management procedures. Throughout the system's lifecycle, risk mitigation must take place.

- Quality and Data Governance: Datasets used for testing, validation, and training must adhere to requirements for completeness, correctness, representativeness, and relevance. The goal of this requirement is to lessen discrimination and bias in algorithms.

- Technical Records: Providers are required to keep thorough technical records attesting to their adherence to the law. Such recordings may be examined by authorities during conformity evaluations.
- Openness and User Data: Users must be given clear instructions so they can comprehend the risks, constraints, and capabilities of the system.

- Human Supervision: High-risk AI systems need to allow for significant human oversight and intervention. When necessary, human operators should be able to override-automatic-judgments.

- Cyber security robustness and Accuracy: Systems must attain suitable levels of technological dependability and resistance to manipulation or cyber-security threats.

- Evaluations of Conformity: High-risk systems must go through conformity assessments to ensure they comply with the Act's criteria before going on sale. CE marking practices are comparable to those found in EU product safety regulations.

The EU's attempt to incorporate product safety concepts into AI governance is evident in the regulatory framework.

Transparency-Requirements-and-Low-Risk-AI-Systems

Some AI systems are less dangerous, but they still have transparency requirements. Examples consist of chat-bots, systems that identify emotions, deep-fakes. When interacting with such systems, users need to be aware that they are interacting with artificial intelligence (AI) instead of people. In order to prevent misinformation and deceit, AI-generated content must also be properly mentioned. As worries about artificial media manipulation during elections and public discourse grew, the deep-fake provisions became more significant.

Low-Risk Artificial Intelligence Systems

The majority of AI applications are classified as low-risk and are still mainly uncontrolled. AI in video games, spam filters, and recommendation systems in everyday situations are a few examples.
In order to prevent overregulation, the EU purposefully took a lax attitude to low-risk innovation.

General-Purpose-AI-Model-Regulation-[GPAI]

Large language models and generative AI systems are examples of general-purpose AI models, which are among the most innovative features of the AI Act. The introduction of Open AI GPT models and other similar systems compelled lawmakers to address fundamental AI technologies with a wide range of downstream applications.
GPAI model providers are required to keep the technical records up to date, to describe the training data, adhere to EU copyright regulations, for highly capable models, perform systemic risk evaluations, put cyber-security measures in place. Concerns regarding innovation, trade secrets, and global competitiveness made the regulation of GPAI models politically controversial. During efforts to lessen regulatory constraints, major tech businesses actively campaigned.

Intellectual-Property-and-Copyright-Concerns

Copyright law and the AI Act have a lot in common. Summaries of copyrighted training materials must be published by providers of generative AI systems. Growing conflicts between AI developers and creators including writers, musicians, journalists, and artists who claimed that protected works were being used without permission for model training gave rise to this need. The EU's current copyright exemptions for text and data mining, according to critics, provide legal loopholes that favour to big AI companies. The unresolved copyright issue could lead to further legal action in European courts.

Mechanisms-for-Governance-and-Enforcement

A multi-layered governance system encompassing national authorities and EU institutions is established by the AI Act.

Office-of-European-AI

Advanced GPAI models are overseen and implemented by the European AI Office. The European Commission oversees its operations.

Authorities-for-National-Supervision

Competent authorities must be appointed by each Member State to oversee and enforce market surveillance.

European-Artificial-Intelligence-Board

THE EU BOARD, encourages uniform application of the regulation and fosters coordination among-the-Member-States.

Sanctions-and-Penalties: Non-compliance with the AI Act carries harsh financial consequences.

Possible penalties consist of: Prohibited AI activities can cost up to €35 million, or 7% of the world's annual revenue, for additional infractions, up to €15 million or 3% of turnover, or the SMEs may be exempt from penalties under specific circumstances. The punitive structure demonstrates the EU's commitment to strict enforcement and reflects the deterrence mentality of the GDPR.

THE-EU-AI-ACT-EVALUATION

The AI Act has drawn a lot of criticism despite its importance.

- Concerns-about-Overregulation: Excessive compliance requirements, according to critics, could burden start-ups and inhibit innovation. Documentation, compliance evaluations, and the legal ambiguity can be one of the challenging factor for the small kind of businesses.

- Enforcement Challenges: Regulators and courts may not be able to handle the technological complexity of AI systems. Highly specialized technical expertise is necessary for effective monitoring.
- Worldwide-Competitiveness: Strict regulation, according to some industry players, can make Europe less competitive in comparison to the US and China.

- Loopholes in Copyright: Inadequate safeguards against unapproved AI training methods are still criticized by the creative sectors.

- Enforcement Challenges: Regulators and courts may not be able to handle the technological complexity of AI systems. Highly specialized technical expertise is necessary for effective monitoring.

3.4THE ROLE AND LIABILTY OF INTERMEDIARIES AND THE SOCIAL MEDIA PLATFORM

Globally, the proliferation of deep-fakes has sparked serious ethical, legal, and social issues. Social media platforms and internet intermediaries play a crucial role in either supporting or restricting the circulation of such modified media because the majority of deep-fake information is disseminated through digital networks. Social networking sites, search engines, internet service providers, video-sharing websites, hosting services, and messaging apps that let users post, share, send, or access content online are examples of intermediaries. Although these organizations don't always produce harmful information, they frequently serve as conduits for it to reach millions of consumers.
Because deep-fakes propagate quickly and have the potential to cause irrevocable harm before they are discovered or removed, the discussion about the accountability of intermediaries and social media platforms has become more heated. As a result, governments and regulatory bodies throughout the world are working to specify the level of responsibility and due diligence requirements that intermediaries must work in order to mitigate the negative effects of deep-fakes.

The role of intermediaries and social media platforms in connection to deep-fakes, their legal obligations, the difficulties in content regulation, and striking a balance between accountability and freedom of expression are all explained in this essay. An organization that helps users on digital networks communicate or obtain information is known as an intermediate. Online platforms that host or transmit third-party content are typically referred to as intermediaries in legal term. Examples are Websites for social networking, platforms for sharing videos, Messaging apps Search engines, providers of cloud hosting, Internet service provider. A particular class of middlemen known as social media platforms enables users to produce,

upload, and share material in a public or semi-public manner. Because they promote quick sharing, interaction, and algorithmic amplification, these platforms have emerged as the main avenues for the spread of deep-fake content.
Because they run the infrastructure that allows deep-fakes to proliferate, intermediaries are crucial. They have the technological capacity to identify, limit, eliminate, or classify corrupted media, even though they might not produce it themselves.

ROLE OF INTERMEDIARIES REGARDING DEEP-FAKE:

Monitoring and Moderation of Content: The Content control is one of the main responsibilities of intermediaries. It is required of social media platforms to recognize and control user-uploaded dangerous information. Intermediaries are increasingly using automated methods and human assessors to identify modified media because deep-fakes can be deceptive ordangerous.
In general, content moderation entails: Keeping an eye on uploads, Reporting questionable content, eliminating dangerous deep-fakes, limiting visibility, suspending accounts for persistent infractions. A lot of platforms use artificial intelligence-based detection techniques that examine irregularities in metadata, lighting patterns, audio synchronization, and facial movements. It is also possible for human moderation teams to check if material is in violation of platform policies.
However, because deep-fake technology is always changing, identification is still challenging. Advanced deep-fakes have the potential to evade automated systems and stay online long enough to do extensive damage.

Due Diligence Requirements: Governments are putting more and more pressure on intermediaries to handle online information with "due diligence." Due diligence is taking appropriate precautions to avoid the distribution of dangerous or illegal content.
In India, intermediaries are required by the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 to notify users about content that is forbidden and to delete illegal content after being notified. The Ministry of Electronics and Information Technology has issued government advisories that have particularly.

It might be necessary for intermediaries to: Disseminate explicit user instructions, create procedures for resolving grievances, eliminate dangerous deep-fakes within the allotted period, assist law enforcement, Continue to provide transparency reports, take reasonable steps to avoid disinformation and impersonation. Therefore, the function of intermediaries goes beyond simply hosting content. It is becoming more and more required of them to take an active role in digital governance.
To protect against False Information: Misinformation and disinformation efforts are greatly aided by deep-fakes. Engaging content is given priority by social media algorithms, which may inadvertently magnify sensationalized edited films and made-up stories. Intermediaries contribute significantly to the decrease of false information by: Verifying the accuracy of dubious media, labelling information that has been altered, lowering the amplification of algorithms, endorsing reliable sources of information, alerting users before to publishing content that is contested.

Certain platforms include cautionary labelling like "altered content," "synthetic media," or "digitally manipulated." Instead of naively believing internet content, these labels assist users in critically assessing its legitimacy. Deep-fakes can affect public opinion and democratic outcomes, therefore this function becomes particularly crucial during elections, public emergencies, and political disputes.

Collaboration with Governmental Authorities: When looking into crimes related to deep-fakes, intermediaries frequently collaborate with law enforcement and regulatory organizations. Platforms may be asked by governments to remove illegal content, reveal user data, or preserve evidence. This kind of collaboration is especially required in situations involving:
Online fraud, Theft of identity, Sexual abuse, Interference with elections, Slander
Dangers to national security.

The advancement of detection technologies: Research on deep-fake detection is highly funded by large social media firms. Platforms must constantly enhance their detection techniques due to the rapid evolution of deep-fake creation technologies. Among the technological initiatives are: Forensic analysis powered by AI, Systems for watermarking, Authentication of metadata, verification via block-chain, mechanisms for tracing sources. Some businesses work with academic institutions and civil society groups to develop industry-wide guidelines for spotting falsified media.

Intermediaries'-Legal-Liability:

Protection of Safe Harbour. The majority of nations offer "safe harbour" protection to intermediaries. Safe harbour refers to the fact that intermediaries are not always held accountable for illegal content that users post as long as they follow the law and take appropriate action after being informed. Intermediaries in India are granted conditional protection under Section 79 of the Information Technology Act, 2000. Only when intermediaries exercise due caution and do not intentionally assist illegal behaviour can they qualify for this safety. Safe harbour is justified by the fact that platforms are unable to effectively monitor all of the billions of user-generated content pieces they contain. Deep-fakes, however, pose a threat to this paradigm since governments are putting more and more pressure on platforms to detect dangerous synthetic media before it becomes widely disseminated.

Proactive Monitoring vs. Actual Knowledge: Whether intermediaries should monitor content proactively or just take action after receiving notice is one of the main legal arguments.
In the case of Shreya Singhal v. Union of India, the Indian Supreme Court ruled that intermediaries must only remove illegal content after obtaining real knowledge through court orders or government notifications. Opponents contend that requiring proactive surveillance could Promote excessive censorship, endanger the right to free speech, increase the burden of compliance, lead to the arbitrary removal of content.
However, proponents contend that proactive monitoring is required because to the rapid proliferation of deep-fake and their potential for imminent harm. The larger difficulty of striking a balance between digital freedom and platform accountability is reflected in this tension.

ROLE AND LIABILITY OF SOCIAL MEDIA PLATFORM:

Despite the fact that many digital entities are middlemen, social media platforms play a particularly significant role due to their algorithmic systems and reach.

Amplification via Algorithms: Social networking sites use algorithms that are intended to increase user interaction. Deep-fake content that is sensational or emotionally charged frequently gets more views, shares, and reactions, increasing its visibility. Platforms may therefore inadvertently aid in the viral dissemination of altered media. Thus, one of their responsibilities is to investigate how harmful content is amplified by engagement metrics and recommendation-algorithms. Platforms can lower this risk by: Restricting the suggestion of content that has been flagged, removing the deceptive videos, Disrupting quick sharing habits
giving credible sources priority.
Platform Policies and Community Standards: The majority of significant social media sites have regulations against impersonation and altered material. In general, these regulations forbid false synthetic media, intimate imagery that is not consented to false information about the election, false impersonation. Platforms use visibility limits, content removal, and account suspensions to enforce these standards. Enforcement is still uneven, though. While genuine satire or parody may be inadvertently removed, some damaging deep-fakes persist online for long periods of time.

Mechanisms for User Reporting: Users can report harmful or questionable content using the tools provided by social media companies. Because automated algorithms are unable to correctly recognize every deep-fake, such procedures are crucial.

Digital literacy and public awareness: Additionally, social media companies have an obligation to inform users about media manipulation and deep-fakes. Initiatives to raise awareness could include: Campaigns for education, fact-checking collaborations, resources for media literacy, alerts regarding the dangers of false information. Because even the most sophisticated moderation mechanisms are unable to totally exclude synthetic media from online spaces, digital literacy is crucial.

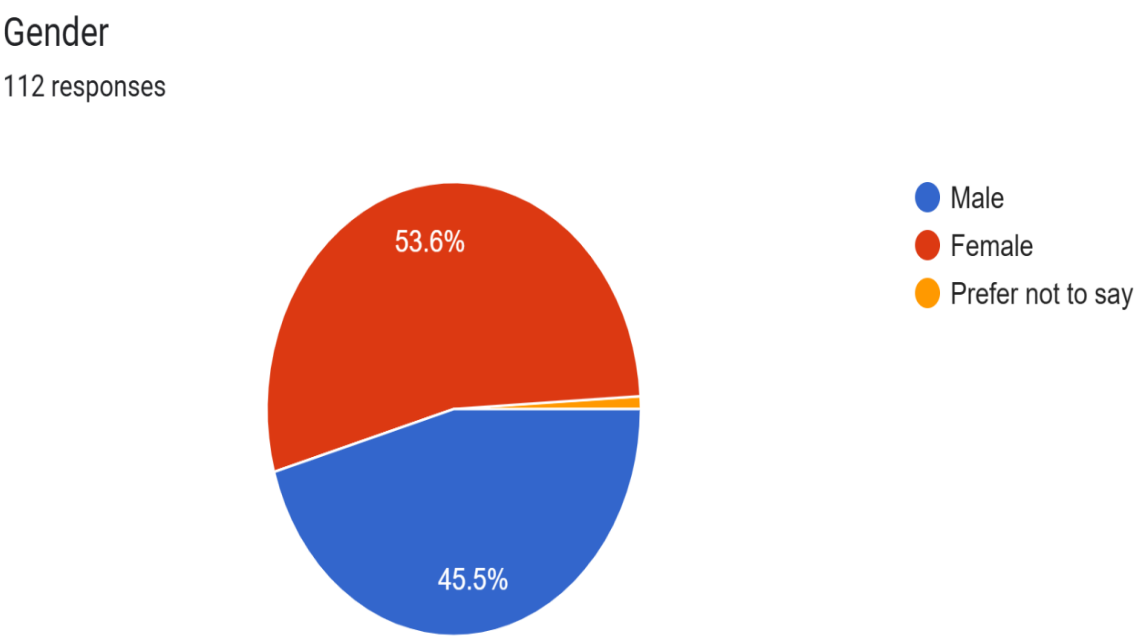
CHAPTER 4: DATA ANALYSIS

This chapter presents the analysis of data collected in this research by the method of "Simple Random Sampling". Here, the total number of responses collected with the help of Google form is 112 and the total number of questions asked from them is 19 including the name of the respondent.

Before analyzing the data collected, I would like to explain why this method of collecting responses is helpful in a research.

- It is helpful to a researcher in understanding the awareness level of the people.
- It is also helpful in analyzing the exposure frequency of the people.
- The digital literacy of the people are also shown while collecting responses.

1. The very 1st response in this survey is regarding the gender of the people participating in this survey.



From the above graph we can conclude the various data:

- The representation of different genders:

Here, the total number of respondents is 112, out of which 53.6% is female which approximately makes a total number of 60 responses. Also, the total percentage of male responses is 45.5% which is nearly making 51 responses.

Now, prefer not to say section is nearly about 0.9% i.e. 1 response.

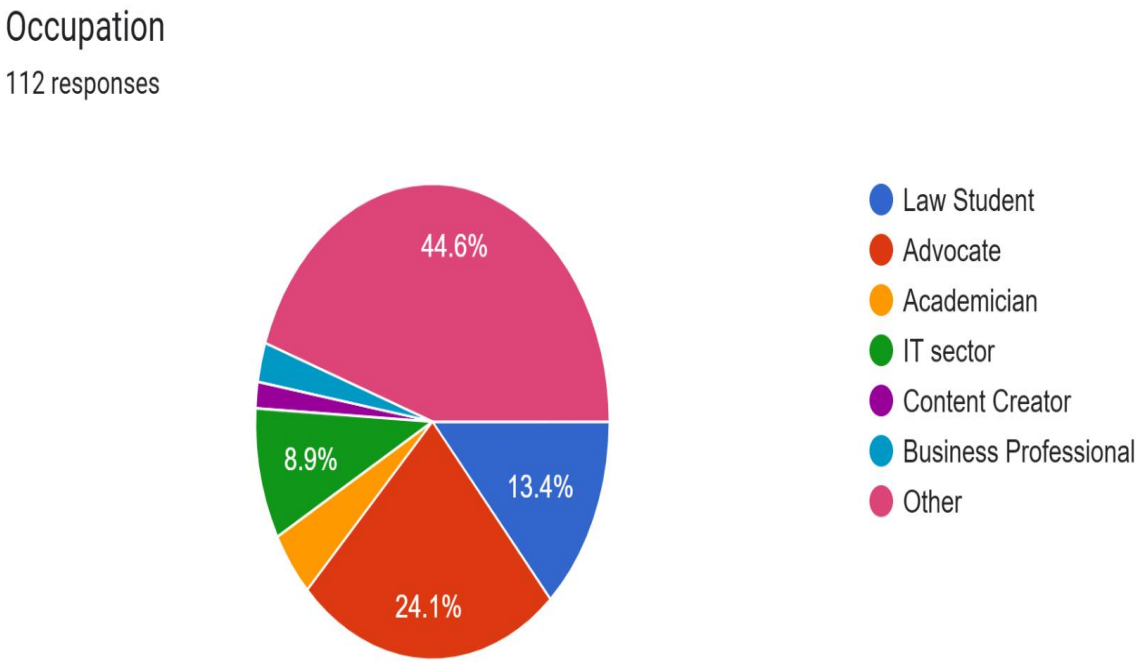
So, we can say that this survey sample is nearly balanced in terms of gender, though it is slightly female dominated. The balanced participation helped in reducing the chances of sampling biasness, gender over-representation, one sided interpretations etc. Also, the balanced gender representation improves the chances of the comparative analysis of both the genders, statistical reliability and the diversity of perspectives.

Here, the gender distribution is helpful in understanding the impact of deep-fakes on different genders like the vulnerability of a gender, societal consequences, fear and awareness, better understanding of the term deep-fake etc.

- Out of 112 responses 1 response shows the option of "prefer not to say" about gender which somewhere may indicate the person's privacy concern, distrust in the data, fear of profiling or may be gender identity sensitivity. It is a very small data but it shows the awareness of privacy.

P.T.O

2. The 2nd response is regarding the occupation of the respondents participating in this survey.



The above Pie-chart shows 7 different categories of professionals involved in this survey. They are broadly classified into Law students, Advocates, IT sector, Academician, Content creator, Business professional and others.

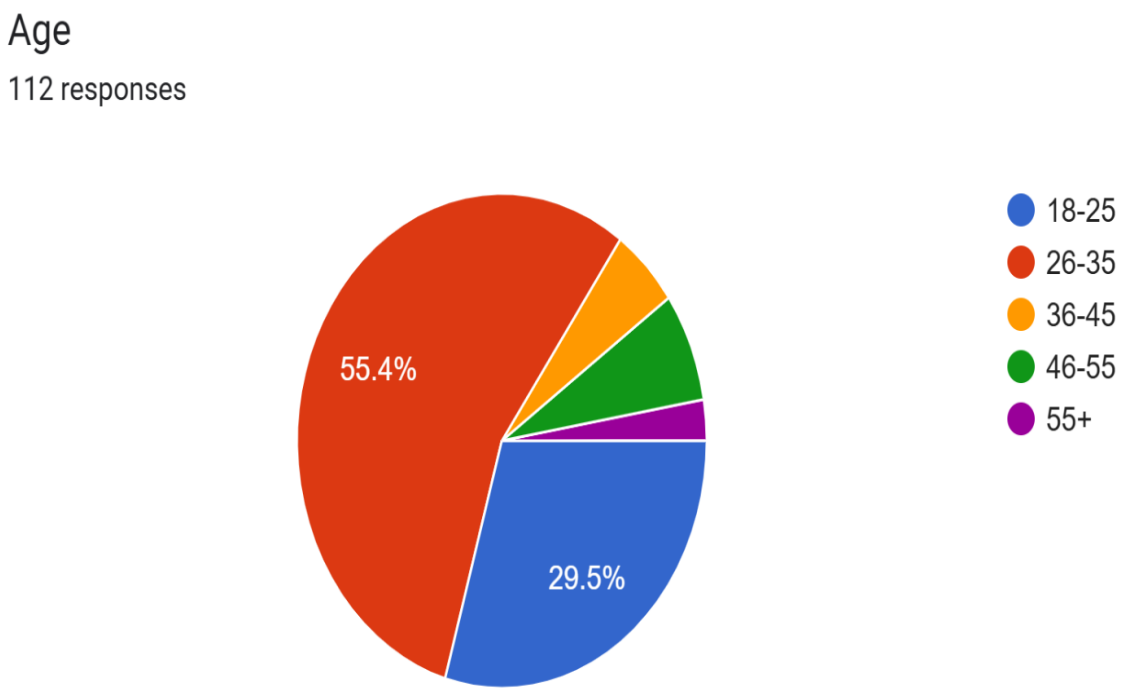
Here, the largest % of responses is under the category of others, i.e. a total of 44.6% of the total which is approximately 50 responses. While, the Advocates are around 24.1% of 112 i.e. nearly there are 27 responses from them. 13.4% are law students which makes 15 responses from them. The IT sector professionals are about 8.9% i.e. there are nearly 10 responses from their side. The Academicians, the business professionals and the content creators have participated in a very small % in the survey yet there data are very much relevant for the survey.

Now, taking data from different kinds of professionals plays a very important role in understanding the fact that how different sectors are affected in different manner due to deep-fake. It also helped us in understanding the knowledge of different professional regarding our existing legal framework and the technological advancement happening out.

The Advocates and the law students might be focused more on the legal perspective while giving responses as they are likely to be more aware about the legal perspective than the other professionals. The responses coming out from the law students shows that the students nowadays, are becoming aware about the advancement of the technology around their surroundings. The IT professionals might have given responses by thinking about the data security in the technological world and also the deep-fakes are created by using the advance technology only and the IT sector professionals are having technical knowledge regarding various kinds of technologies. For the business professional the reputation risk and cyber

fraud could be the main concern while giving responses, there are more chances of them to be a victim of intellectual property deep-fakes. Although, in this survey the content creators are very few in numbers but in their profession deep-fake plays a very important role for example: It can be used in generating voices in different languages, satire, story-telling etc. Also, the percentage of Academicians is also very low in this survey yet very important as they can response very well this issue analytically and ethically. Now, the largest response was from the group Others, which shows that the issue of Deep-fakes is not only limited to certain specialized professions only but it has become a concerning topic to the people at large.

3. The chart shows the ages of the respondents of the survey:



The age group is divided into 5 categories, i.e. 18-25, 26-35, 36-45, 46-55, 55+. In which 18-25 is 29.5% which shows approx. 33 responses are from this group, 26-35 is 55.4% i.e. 62 responses are from this group only, 36-45 is less in number, 46-55 is 7.1% which indicates that nearly 8 responses are from this group only and 55+ has very few responses.

From the chart we can analyze the fact that the maximum number of responses are coming from the young generation while the older age group's contribution is very low. Also the highest number of responses are from the age group 26-35, which shows the young adults had given more than half of the responses. The people of this age group are the young adults who are highly active on social media platform as well as they are ones working with the technology also and because of the very same reason this is the age group who more likely to be exposed to the highly generated synthetic videos, photos, misinformation etc. Their participation in such a huge percentage shows that the topic of deep-fake is somewhere related to their day to day stuffs as they share and receive online contents regularly.

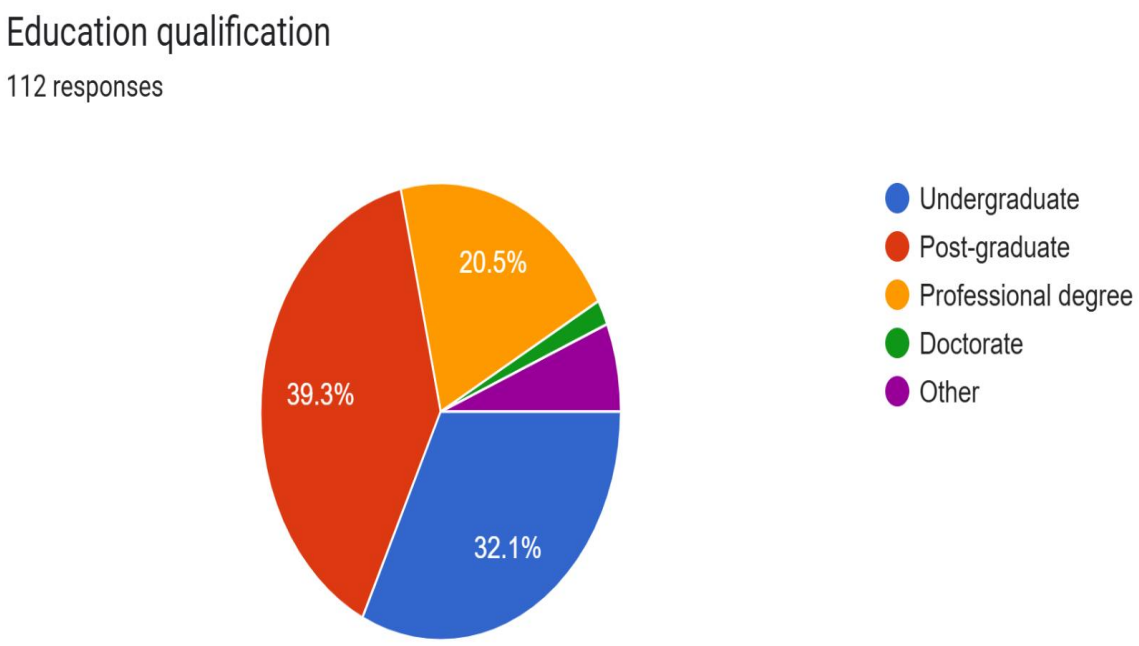
Now, the 2nd highest response is from the group 18-25, which is mostly considered to be the group of young students, recent graduates who are basically young internet users.

From the above two groups we get to know that nearly 85% of the total response is from the young generation only in this survey which shows their dominance in the field of technologies as they are the ones who are the creator as well as the adopters of the technologies. And because of the very same reason they are the ones who will encounter the most use of deep-fake on several platforms.

Also, as we have seen that the survey response is 85% given by the youth which shows that it will likely reflect the opinions of the youth population more as compared to the older generation.

The 3rd largest group is from the age 46-55, which is nearly 7.1% of the 112 i.e. 8 responses from this group, which shows the survey has limited exposure to the middle aged people. Also they may have less technological exposure also which makes them a soft target of digital manipulations like deep-fakes etc. Another major reason of their participation in less quantity is due to digital illiteracy in that generation, also lack of awareness program regarding technological enhancement in the age group.

4. The 4th pie-chart shows the educational qualifications of the respondents.



Here the educational qualification of the respondents is classified into five different categories: Undergraduate, Post graduate, Professional degree, Doctorate, Others. Now we can see that the total percentage of undergraduate respondent is 32.1%, the highest % is of Post graduate which is 39.3%, also the percentage of Professional degree respondent is 20.5%, here, the total number of doctorate is only 2 while the percentage of respondents with other type of degree is 6.3%. So from the above given pie-chart we can conclude that the sample collected is of academically very diverse background. Here, from the chat the maximum responses are from the respondents having higher educational qualification. On the 2nd place lies the responses of the undergraduate respondents, which shows that the research will reflect us the thinking of the younger generation as well as the academically engaged individuals. Also, the least number of response is from the academically expert individuals like the doctorate, which reflects that the research focuses more on normally academically sound people rather than the expert ones in the field.

Now, from the data collected we can calculate the total number of respondents from each particular qualification category, i.e. the undergraduates are 32.1% which makes them about 36 number of respondents, the Post-graduates are having a 39.3% of the total i.e. they are approximately 44 in number, the responses from the professional degree is a total of 20.5% which makes them nearly 23 in number, the least number are responses from the doctorate which makes them a total of 1.8% i.e. 2. The last category of qualification was others which was a total of 6.3% i.e. 7 responses are from that category.

Here, when we will the 3 major categories% we will get to know that they together had given more than 90% of the responses, which indicates that the responses are majorly collected from the people having greater exposure of technology and are having higher academic knowledge.

SEPARATELY ANALYZING EACH CATEGORY:

i.UNDERGRADUATE CATEGORY:

It represents mostly the younger generation people who are using technology in their day to day life or we may say that they are digitally active ones. In today's generation they are active on social media platforms like Instagram, Snapchat, X, Facebook which is one of the major platform where the deep-fakes are circulated rapidly. Therefore, the study of this generation helped in finding their encounter with deep-fakes like memes etc. whether they are circulating it or not. They are having a very practical exposure to the synthetic media like deep-fakes as they are very much familiar to the technology.

ii.POST-GRADUATE CATEGORY:

In the chart the maximum responses are from this category only. Now, the responses from this category are from the individuals who are having higher research knowledge as well as they are having more awareness about the technological developments. The chances of them having familiarity with the technology is high also, there are chances that they may be having more academic discussions about AI, Machine Learning, Deep-fakes etc.

iii.PROFESSIONAL DEGREE CATEGORY:

In this chart the 3rd largest responses are from this category only. Now, this group consists of various professionals from very distinct fields like Engineering, IT, Media etc. Their participation helped in knowing the perspectives of the individuals from different practical background.

iv.DOCTORATE CATEGORY RESPONSE:

The participation of this category is very low as compared to the other category in this survey but their response still holds a very significant value in this study as they are the ones having strong theoretical as well as analytical knowledge, which makes them the individual having advanced research skills for answering and knowing any concept.

v.OTHER CATEGORY:

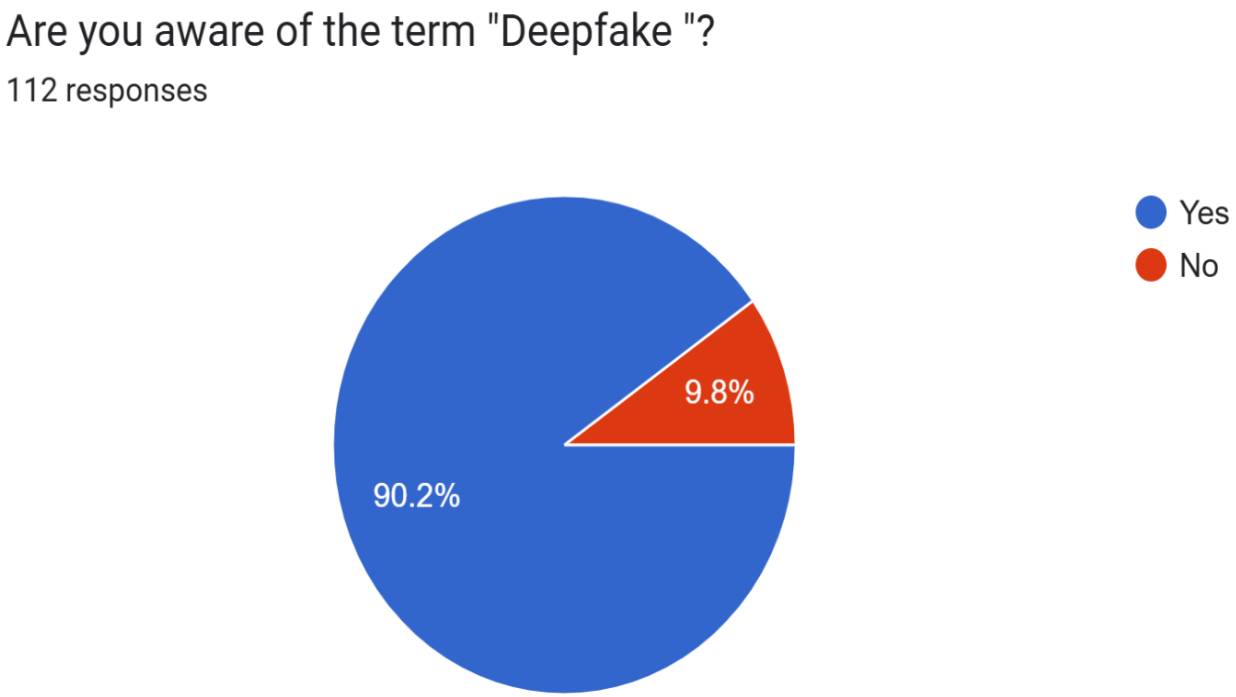
It represents various categories like the one having diploma, vocational course, self-taught individuals etc. The response of this category is important because the synthetic media like deep-fake is not affecting the individuals by knowing their educational background. The one who is not having exposure to the changing technology are more vulnerable to the technology like deep-fake.

vi.OVERALL IMPACT OF EDUCATIONAL BACKGROUND OF THE RESPONDENTS ON THIS RESEARCH:

The individuals having significant education will be able to perform critical thinking before answering the questions. Also, they will be more aware of the technological reform happening around them.

P.T.O

5. **The 5th response shows the understanding of the term Deep-fake by the individuals, i.e. whether they are aware of the term "Deep-fake" or not.**



This chart shows the positive response % is around 90.2% which is approximately 101 responses while, the negative response is around 9.8 i.e. around 11 responses out of 112.

Now, the question regarding the awareness of deep-fakes shows the technological literacy of the individuals, their digital exposure and their experiences with AI. Also, from the survey it is clear that more than 90% of the samples are aware about this which shows people are now being aware about the penetration of AI in social environments.

The social media platforms like Whatsapp, X, Instagram etc are one of the major circulator of deep-fakes. But to these platform people are also becoming aware about this type of synthetic media. We can easily see that there are 100s of deep-fake photos, videos etc. of public figures like actors, politicians are spreading on everyday basis, which had made aware even the individual who is not having technical knowledge regarding deep-fake. This chart also indicates that AI manipulations like Deep-fake have now reached to the discussion level of public conversations.

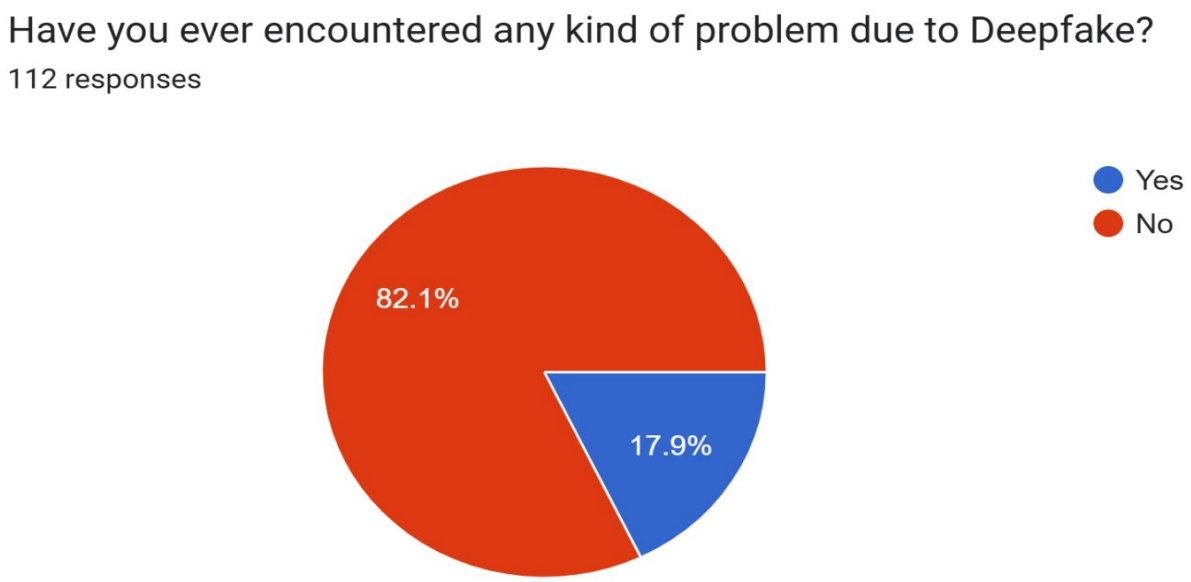
Here in the pie-chart above 9.8% is negative response, which concludes that till date the society had not become a technologically educated society. Approximately 1/10 of the population is still not aware about the Deep-fakes, which shows technical or digital knowledge gap in the society.

These responses highlights the inequality in technical awareness in the society and awareness is the basic need for protection against the misuse of the technology.

We are living in the era where digitalization had become a part of our day to day life, and if the people living in this era would lack in understanding the manipulated videos, photos, audios it will influence the outcomes of elections, can damage the reputation of the individual in the society, can enable cybercrime to a very large extent.

P.T.O.

6. The Next Response Is Given Below:



Here, we can see that 82.1% of the responses are clearly indicating that they have not encountered any kind of problem due to deepfake while the rest 17.9% had given the response that they have encountered any kind of problems regarding the deep-fake.

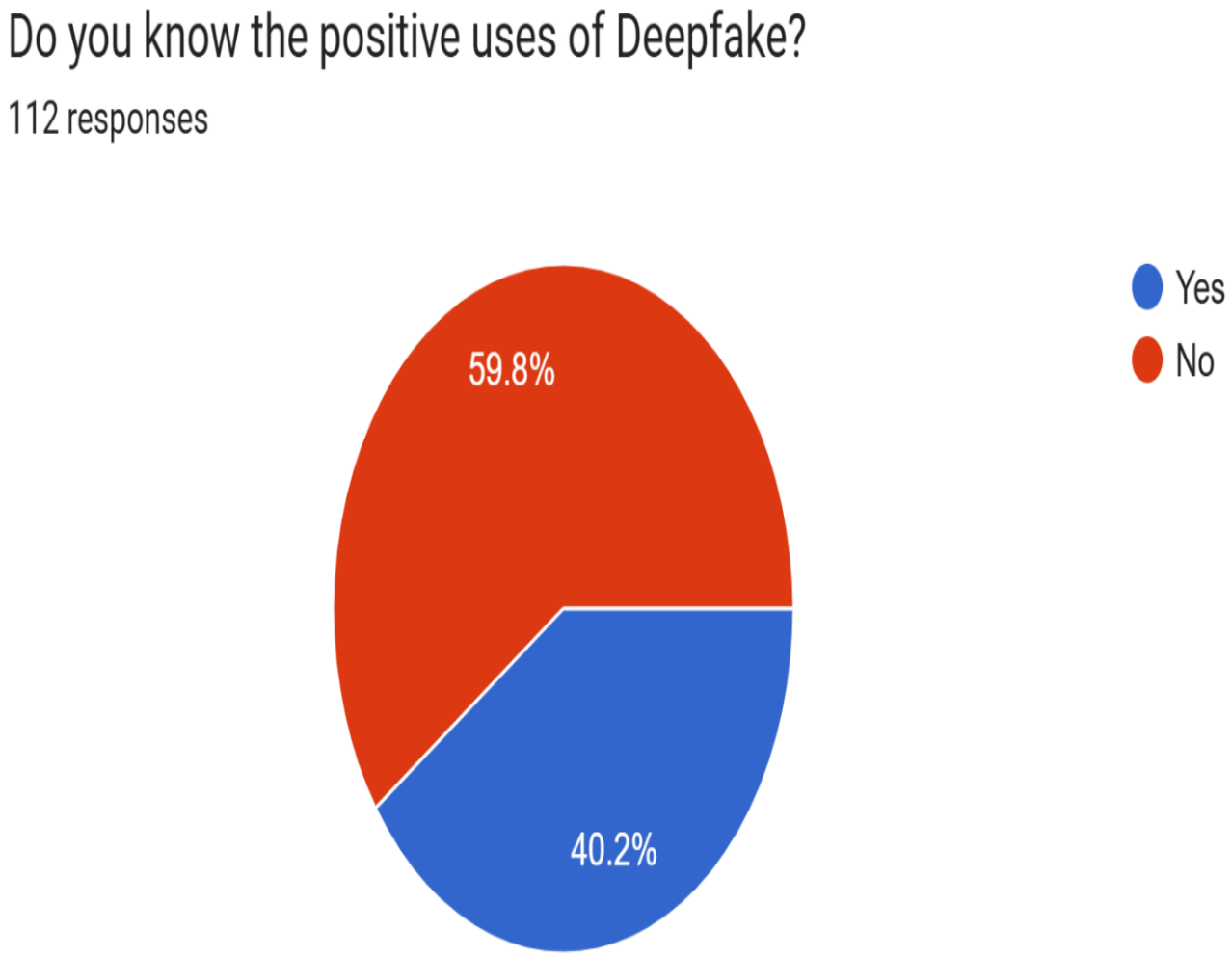
Breaking down the % into numericals we get to know that approximately 92 individuals had given the negative response regarding experience of deep-fake problems while 20 individuals had given positive response of having experience of deep-fake problems, this shows that approximately 5 out of 28 people had experienced the deep-fake problem which shows that it had now become a concern for the people at large.

Now, there are a lot of problems that respondents might have faced due to synthetic media generation of deep-fakes like in today's digital word people casually forwards the memes created with the help of deep-fake for entertainment. Also, it is very common cyber crime practice of defrauding an individuals by taking help of the AI generated voice of their known people.

If we notice around our sorrundings we will find a lot of small vendors using the AI generated photos of the celebraties for the endorsement of the product they are selling.

In the pie-chart given above we notice that majority of individuals had given responses that they have not encountered any kind of problem due to deep-fake, it is possible that they might not be aware about what deep-fakes actually consists of which means that they might have believed any content to be true while failing to recognise it's true authenticity. Or as we know, that India is a developing country so till date it is not feasible for everyone to access technology easily, so this might be the reason behind their limited exposure towards deep-fake technology. Another reason could be that there might be awareness among individuals to avoid the problems created due to deep-fakes.

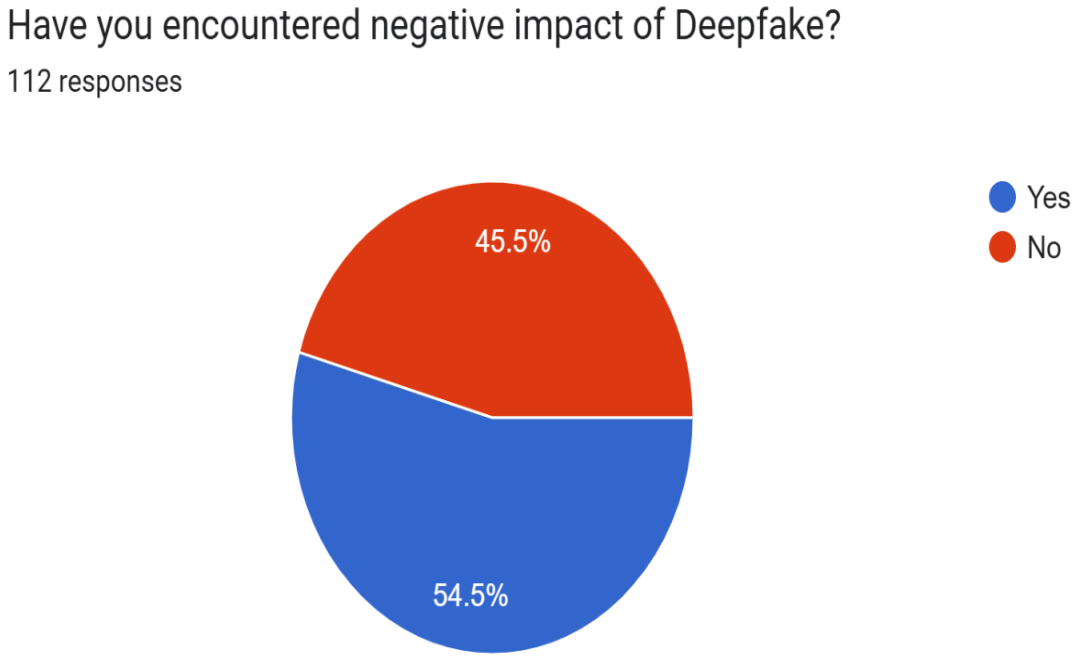
7. The Below Is The responses Collected For The7th Question Of The Survey.



From the above given pie-chart we can analyze the fact that 40.2% of the responses are accepting the fact that they are aware about the positive use of deep-fake, while on the other hand 59.8% of the people are not aware about the positive use of deep-fake. 40.2% of 112 constitutes about 45 responses while 59.8% constitutes nearly about 67 responses. Here, more than 50% of the responses are showing that they are not aware about the positive application of deep-fake, one of the major reason for this can be the marketing of deep-fake technology by the media is highly negative. To make the people aware they had created a panic situation in the mind of the people regarding the new generation AI technology.

There are several positive uses of deep-fakes, like in the entertainment industry it is used for translating as well as dubbing the languages of the movies etc. while in education sector with the help of deep-fakes the visualization of the theories had become a great help in making the students learn the theories easily and effectively. Also in the healthcare industry it is used to help the patients who are dealing with loss of speech and are having neurological problems.

8. Below Is The Response Of The 8th Question Of The Survey:



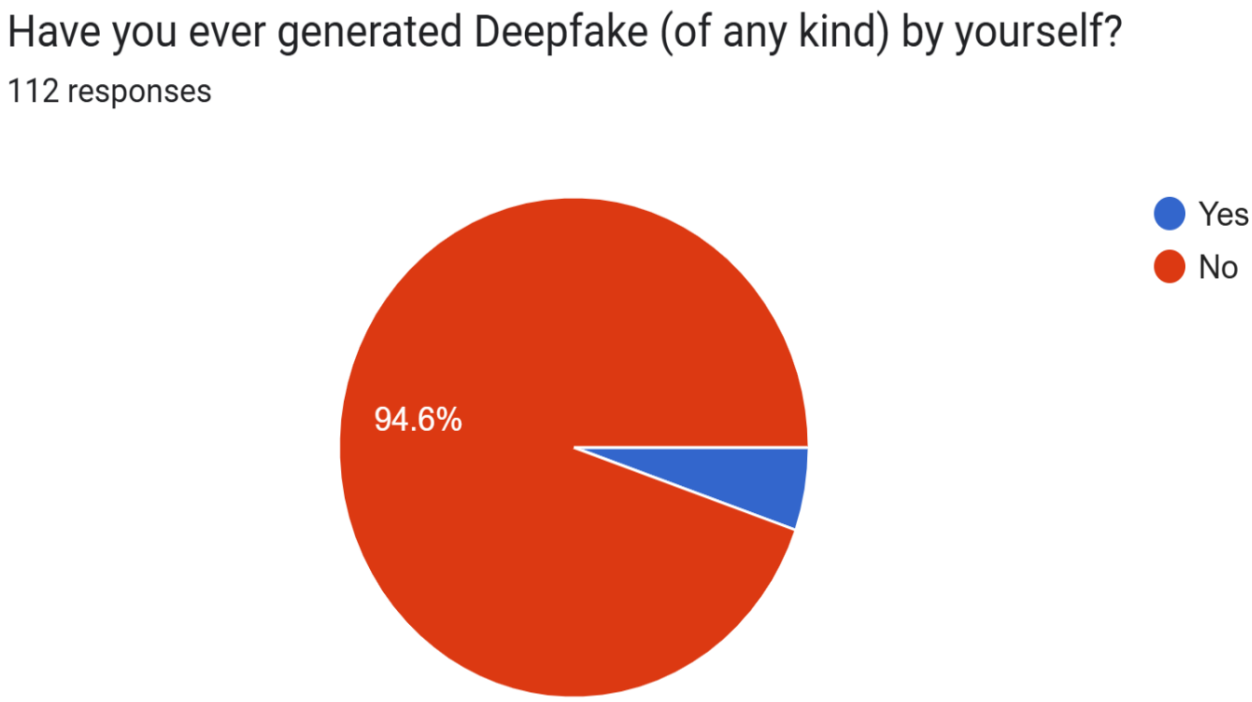
From the above pie-chart we can conclude that 54.5% of the responses, i.e. nearly 61 responses among 112 are stating that they encountered negative impact of deep-fake while the rest 45.5% i.e. 51 responses out of 112 responses are stating the fact that they have not encountered any type of negative impact of deep-fake in their life. Here, we can see that the difference between the two responses is not very high, still the majority respondents had experienced something negative regarding deep-fakes. From the chart responses we can say that the negative functioning of the deep-fake had been experienced by a significant number of individuals in the present digital word. We may assume that the ones who had said that they had experienced might have experienced it through the medium of social media platform, fake calls for financial frauds, fake media contents etc.

Now, in this chart more than half responses are saying that they had experienced something negative from deep-fakes, which shows that how our society had started normalizing the negative effects of AI technologies like deep-fakes. But, the positive responses to this question also suggests that the individuals are now becoming aware in understanding the deep-fakes, which is beneficial for the betterment of our society.

The 45.5% of the responses who had said that they had not encountered the negative impact of deep-fakes is relaxing as well as concerning at the same time. As because it may be the incident that the one who are saying that they had not encountered the negative impact are the ones who is not having proper technological knowledge to identify between the original content or the AI generated ones. India is a country of villages and is still in a position of developing country thus, the digital literacy had not reached to the villages to a certain recognizable extent, so we cannot say that the people living there are free from the negative impact of the deep-fakes, in reality they are the ones who are not able to identity between synthetic media like deep-fakes, in short they are the real suffered ones.

P.T.O

9. Below Is The Pie-Chart Of The Responses Of The 9th Question :

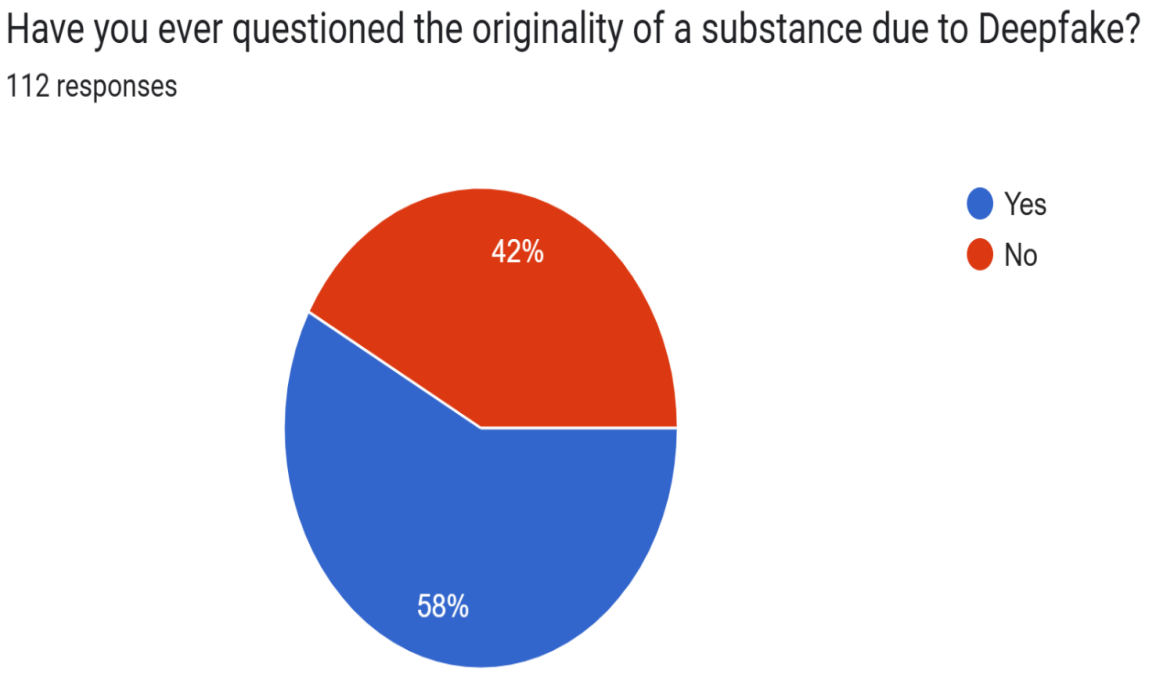


From the piechart we get to see that 94.6% responses are stating that they have not generated any kind of deep-fakes by themselves i.e. approximately 106 number of individuals out of 112 had stated this fact which is a huge response in a particular side. It plays an important role in understanding that using and circulating AI is very easy when compared to creating an AI based content. People still are not that much technologically sound that they can easily generate AI used content of deep-fakes.

There is also a possibility that few respondents had given false review that they have not generated deep-fakes of anykind because of the fear that deep-fakes are generally considered negative in the market, as most people are aware of deep-fakes due to the awareness programmes by the media etc.

Also there is a small percentage of responses i.e. 5.4 % of the total is stating the fact that they have created deep-fakes which is significantly a very low response. It highlights the difference of consumption of technology vs. creation of technology. But we cannot deny the fact that the use of technology is increasing at a very speed and day by day AI is becoming very handy to the people, so the sudden growth of AI can be possible.

10.Below Is The Responses Collected From The Samples On Question number 10 of the Survey:



From above we can analyze the fact that 58% of the responses i.e. a total number of 65 responses out of 112 respones, which is more than half of the responses is stating the fact they they have encountered the situation where the originality of the substance comes into question due to deep-fakes. As the individuals are concerned about deep-fakes, the vast majority of people no longer believe that what they see or hear online is authentic. Just 42% of people still accept digital content at face value. This suggests that a culture of mistrust and uncertainty has grown as a result of deep-fakes. Artificial intelligence and machine learning techniques are used by deep-fake technology to change audio, video, or photos so realistically that it becomes challenging to discern between fake and real information. Deep-fake technology has already started to erode public trust in digital information, as evidenced by the fact that over half of the respondents voiced doubt.

This outcome is quite important from a legal standpoint. Evidence, authenticity, credibility, and truth are the fundamental foundations of law. Digital evidence, including voice recordings, photos, videos, and electronic documents, is frequently used in court to establish justice and liability. However, the validity of such evidence is threatened by the growing frequency of deep-fakes. Electronic recordings may lose some of their evidentiary value if people start to question the authenticity of digital content. Laws pertaining to cybercrime, data protection, evidence, and privacy rights are all affected by this.

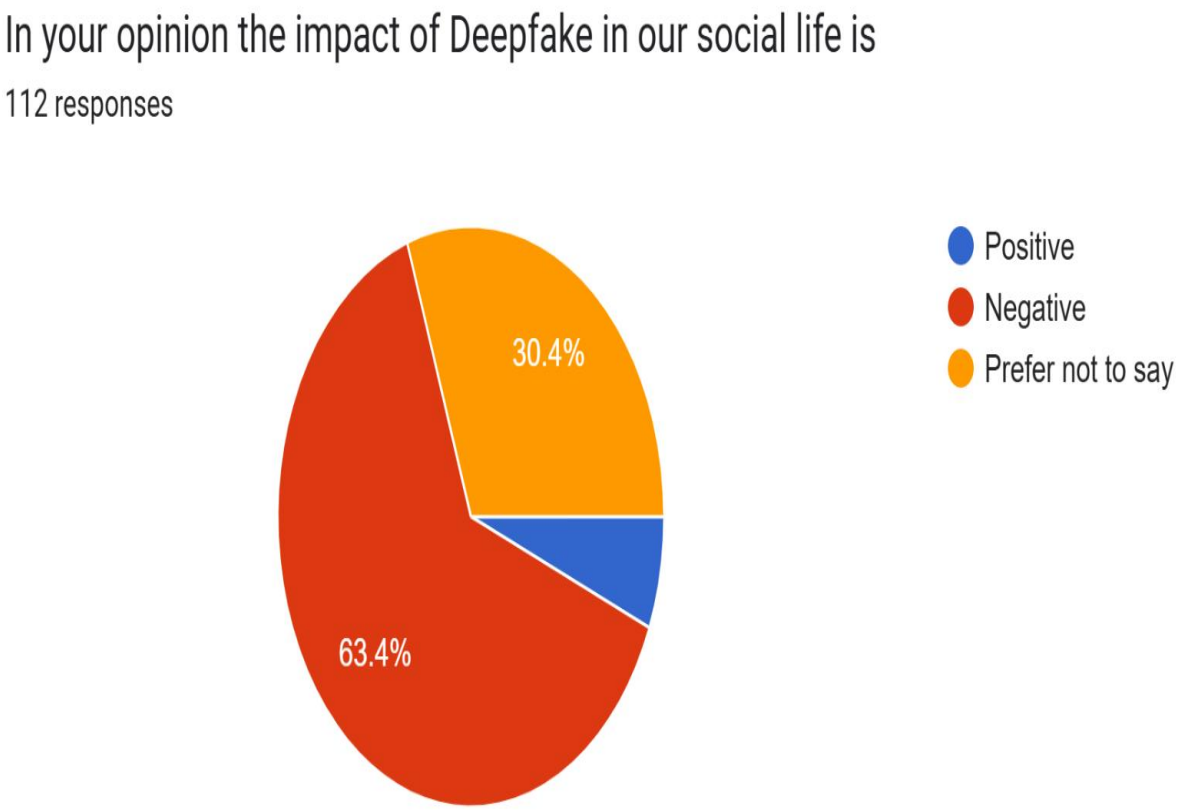
The survey's findings emphasize the critical need for more robust regulatory frameworks to control deep-fake technology in the context of legal research. Deep-fake production and abuse are still not specifically addressed by law in many nations. Current cyber laws may penalize identity theft, fraud, impersonation, and defamation, but they might not sufficiently address the complex harms brought about by AI-generated manipulations. As a result, legislators should think about enacting specific laws addressing the production of deep-fakes without authorization, their malicious distribution, and digital impersonation.
The public's increasing knowledge of technology manipulation is also reflected in the 58% response. This awareness might be seen favourable since it shows that consumers of internet information are become more careful. The capacity to critically analyse digital content is crucial in a time when social media and quick information exchange rule the day. But too much doubting can also lead to social issues. People may become confused, misinformed, and lose faith in media organizations, governmental communications, and legal procedures if they start to question every piece of digital proof.

Analysis of the 42% of respondents who selected "No" is also crucial. Despite the presence of deep-fakes, this segment of the populace either believes that substances are authentic or may not be sufficiently informed on the technology and its consequences. This statistic implies that a sizable segment of the populace continues to rely on digital content without any scrutiny. People who have this kind of trust may be more susceptible to frauds, digital fraud, propaganda, and false information. From a policy standpoint, this highlights the necessity of legal literacy and digital awareness initiatives to teach people how to spot modified content.

In terms of ethics, the graph represents a larger dilemma of authenticity in the digital era. Human communities rely on communication that is honest, trustworthy, and credible. By making it harder to distinguish between fact and fiction, deep-fake technology undermines these ideals. People are becoming more doubtful of what they see and hear online, according to the study results. Such ambiguity can erode interpersonal trust, media credibility, and democratic discourse.

The pie chart illustrates how the public's confidence in the uniqueness and legitimacy of digital content has been greatly impacted by deep-fake technology. While the 42% response shows that a sizable portion of society still retains confidence or is unaware of the risks associated with deep-fakes, the majority response of 58% suggests widespread concern and doubtfulness regarding the surrounding manipulated information.

11.GIVEN BELOW IS THE RESPONSE OF QUESTION 11 OF THE SURVEY:



From the above given pie-chart, we get to see that 63.4% of the respondents are saying that deep-fake had negatively affected their life. 30.4% are the individuals who are may be not in a condition to understand the impact of deep-fake into their lives. 6.3% are the responses which are focusing on how it positively affected their life.

Now, majority responses are negative:

The majority of respondents on the chart i.e. 63.4%, think that deep-fakes negatively affect social interactions. This suggests that the majority of respondents are worried about deep-fake technology's negative implications. This opinion could be supported by the following:
-The propagation of false information and fake news, online fraud and scams, harassment and cyberbullying, reputational harm, a decline in faith in digital media

The smallest percentage is of the positive impact:

Just 6.3% of respondents believe deep-fakes are beneficial. This is the chart's smallest segment, indicating that relatively few people have a positive opinion of deep-fakes. Supporters of deep-fake technology may think it can be helpful in the following areas: creative media production, education and training, entertainment and filmmaking, and technological innovation.

Uncertain or Neutral Reactions.

Prefer not to say; about 30.4% were chosen. This represents a sizable percentage of responders. It might imply that a lot of people are unsure about deep-fakes' effects, don't know enough about the technology, and have conflicting views on its advantages and disadvantages.

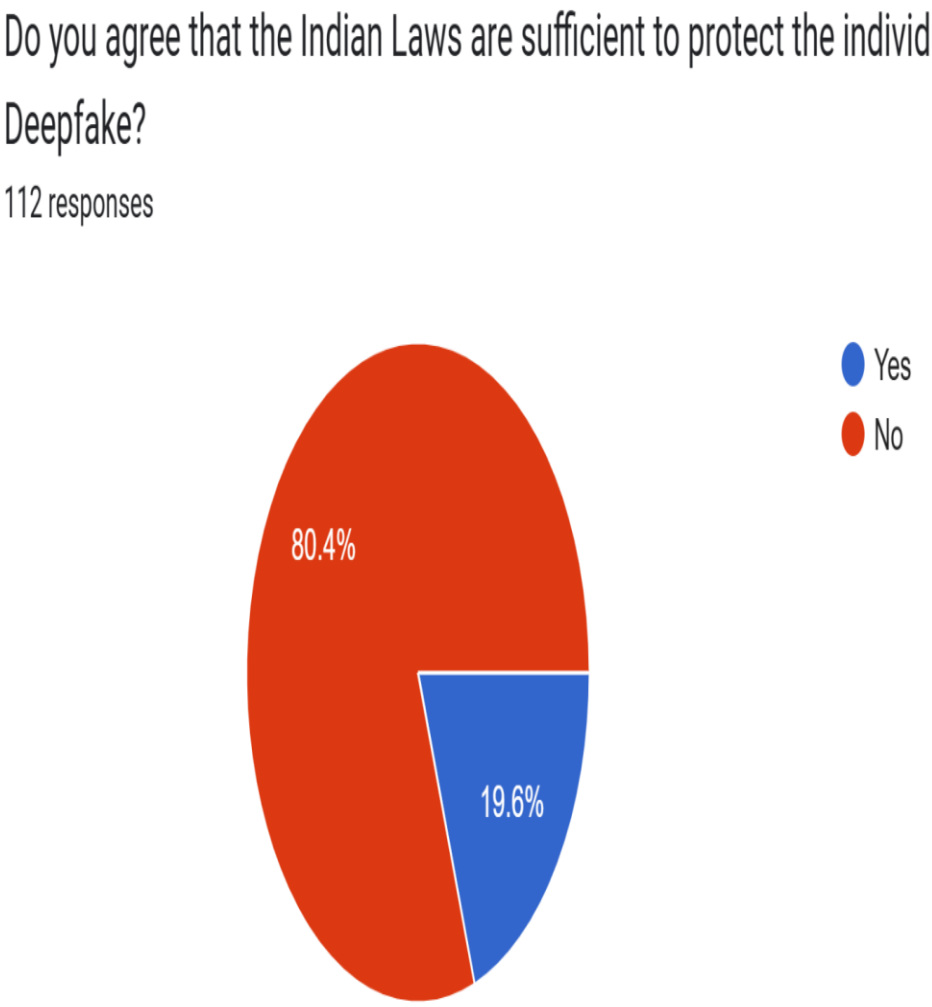
Overall Interpretation of this graph.

The graph unequivocally demonstrates how the general population views deep-fakes negatively. While the majority of respondents identify deep-fakes with social hazards rather than advantages, a sizable portion of respondents were unsure, indicating the need for:

Increased public knowledge, instruction regarding deep-fake technology, moral guidelines, and online safety precautions. Also, the pie chart shows that just a small minority of respondents view deep-fakes favourably, while the majority believe they are detrimental to social life. Many people are still unsure, which suggests that knowledge and comprehension of deep-fake. technology are still evolving. In general, the data shows that people are becoming more concerned about the social repercussions of deep-fakes.

International Journal of Science, Strategic Management and Technology
Volume **02** Issue **05** May-**2026** | ISSN: **3108-1762 (Online)** | Impact Factor: 3.8
An International, Peer-Reviewed, Open Access Scholarly Journal Indexed in recognized academic databases

12.Below is the responses collected on question number 12 of the survey:



From the above given graph we get to the see that majority of the responses that is approximately around 80.4% are stating the fact that the Indian laws are not sufficient enough to protect them from technologies like deep-fake. The graph indicates a widespread belief among the public that India's current legal system is insufficient to deal with the escalating threat posed by deep-fake technology.

The overwhelming negative reaction suggests that people are becoming more concerned about the abuse of synthetic media and artificial intelligence. Deep-fake are capable of incredibly realistic video, audio, and image manipulation, posing concerns like: Identity theft, cyberbullying, revenge pornography, political disinformation, fraud, impersonation, and defamation.

According to the comments, respondents believe that present Indian regulations are ineffective at preventing or correcting these damages.

Also, the responses suggests that: Inadequacy of the Current Legal System

At the moment, deep-fakes are not specifically regulated by any laws in India. Rather, authorities depend on many clauses found in current statutes, like:

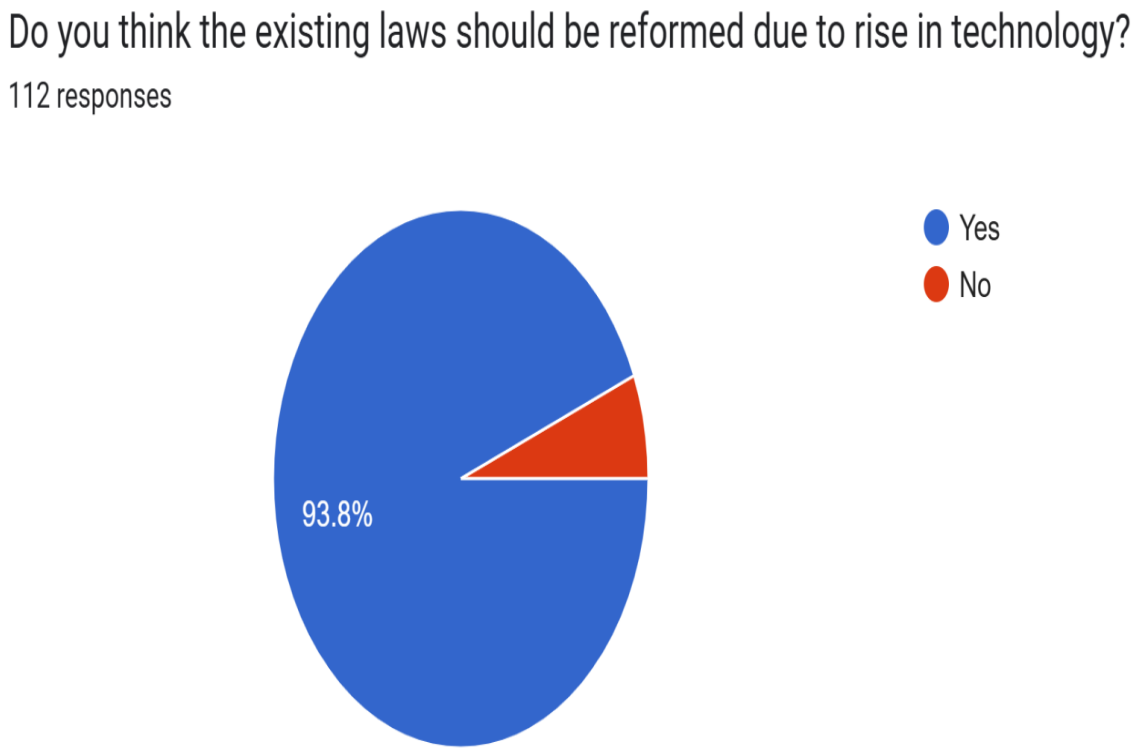
The Indian Penal Code [BNS], copyright rules, data protection and privacy principles, and the Information Technology Act of 2000. These regulations, however, were not initially intended to deal with distorted information produced by AI.

Respondents probably believe that these regulations are inadequate for the quick evolution of technology, difficult to apply in digital environments, and reactive rather than preventive.

Demand for Particular Law.
The high proportion of unfavourable answers suggests that society is in need of:
Legislation specifically designed to combat deep-fakes, hefty fines for producers and distributors, required labelling of AI content, Accountability of the platform, quicker methods for redressing cybercrime and more robust methods for compensating victims.
In the absence of a comprehensive legal framework that particularly addresses AI-generated fraud, respondents probably feel that fragmented regulations are insufficient.

This graph shows a wider problem of faith in digital media administration in addition to legal discontent. Citizens fear election manipulation, reputational harm, online abuse of women and children, and the dissemination of false information and evidence as deep-fake get more sophisticated.
Thus, the data emphasizes how urgently legislators, courts, and regulatory agencies must update cyber laws to reflect new technologies. The pie chart makes it abundantly evident that a sizable majority of respondents don't think Indian laws can sufficiently shield people from deep-fake abuse.

13. The below given pie-chart shows the responses collected on question number 13 of the survey.



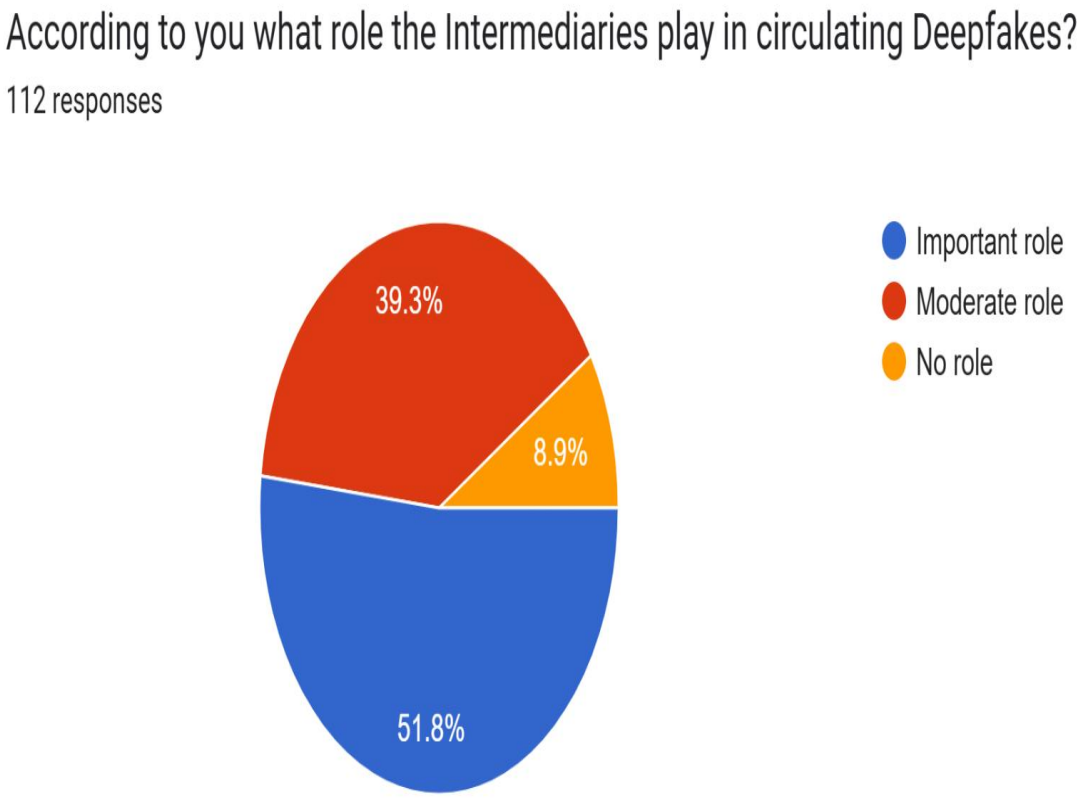
From the above given pie-chart we get to see that the strong support is given in % of responses for the reformation of the laws regarding the new technology.

Only 6.3% of respondents said "No," compared to 93.8% who said "Yes," according to the data. This demonstrates that the vast majority of people think that the current legal system is inadequate to deal with the quick development of contemporary technology and its effects on society. This outcome emphasizes the growing worry regarding the discrepancy between established legal frameworks and new technology advancements including cybercrime, artificial intelligence, data privacy,

digital transactions, and social media regulation. Modern technology challenges may not be sufficiently governed by laws passed decades ago. In order to guarantee justice, security, and the protection of rights in the digital era, the majority view shown in the chart is in favour of new laws, regulations, and updated regulatory frameworks.

The extremely small portion of respondents who were against reform might think that current laws are already sufficiently adaptable due to judicial precedents and interpretation. They make up a very small percentage, nevertheless, when compared to those who support change.

Overall, the pie chart shows an almost uniform agreement that legal systems need to change in tandem with advancements in technology. It implies that society expects legislators and legal organizations to implement changes that can successfully control technology advancements while defending people's rights, the public interest, and moral principles.
14.Given below is the responses collected of question number 14 of the survey.



From the chat we can see that the responses are divided into three categories i.e. No role (8.9%), Moderate role (39.3%), and Important role (51.8%).

The majority of respondents (51.8%) think that middlemen are crucial in the spread of deep-fakes. This illustrates the general public's belief that social media sites, search engines, messaging apps, and hosting services play a major role in the propagation of altered digital content.
Legally speaking, this reflects increased worries about intermediaries' accountability under information technology rules and cyber laws.

39.3% of respondents, a sizable portion, think intermediaries have a moderate influence. This suggests that although platforms aid in circulation, users and content producers who purposefully create or distribute misleading content may also have the main responsibility.

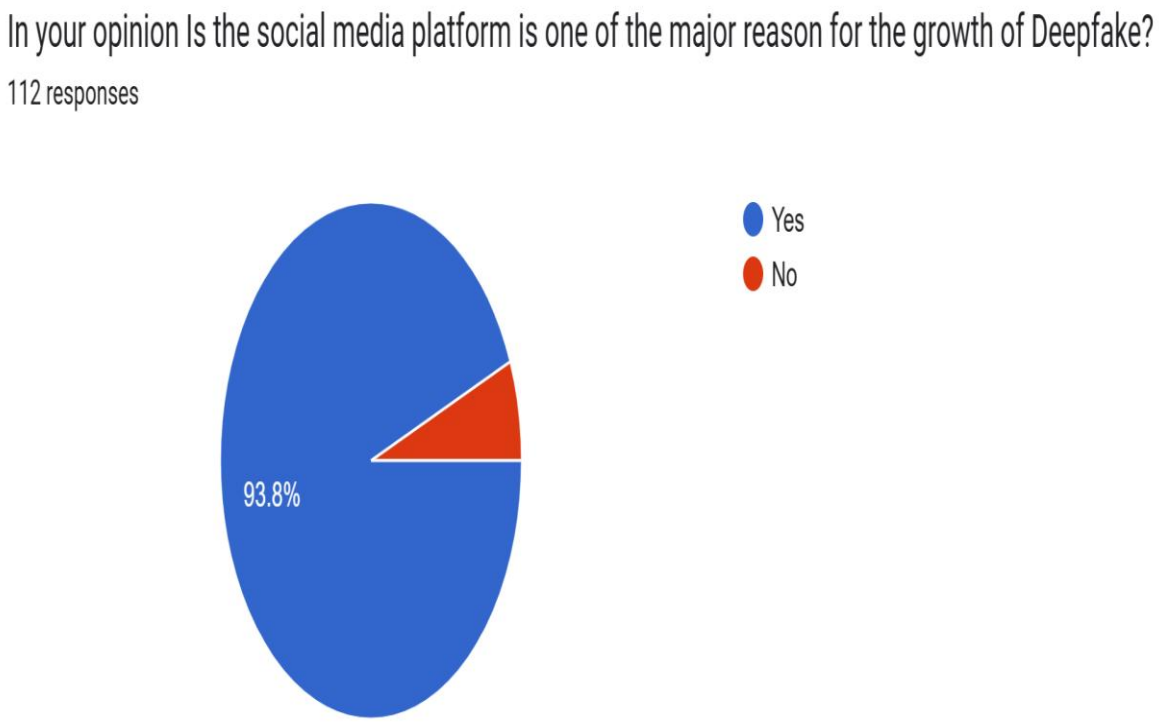
This illustrates the legal concept of shared liability, which divides accountability among up-loaders, hosting companies, and producers.

Just 8.9% of respondents think intermediaries are not involved in the spread of deep-fakes. This minority opinion might lend credence to the claim that, absent actual knowledge of illegality, intermediaries should not be held accountable for user-generated content because they only supply technological infrastructure. This line of thinking is consistent with the "safe harbour" notion that is acknowledged in most jurisdictions, including clauses found in information technology laws.

The chart subtly highlights the need for more robust regulatory frameworks addressing online harm and digital manipulation since respondents primarily link intermediaries to the dissemination of harmful content.

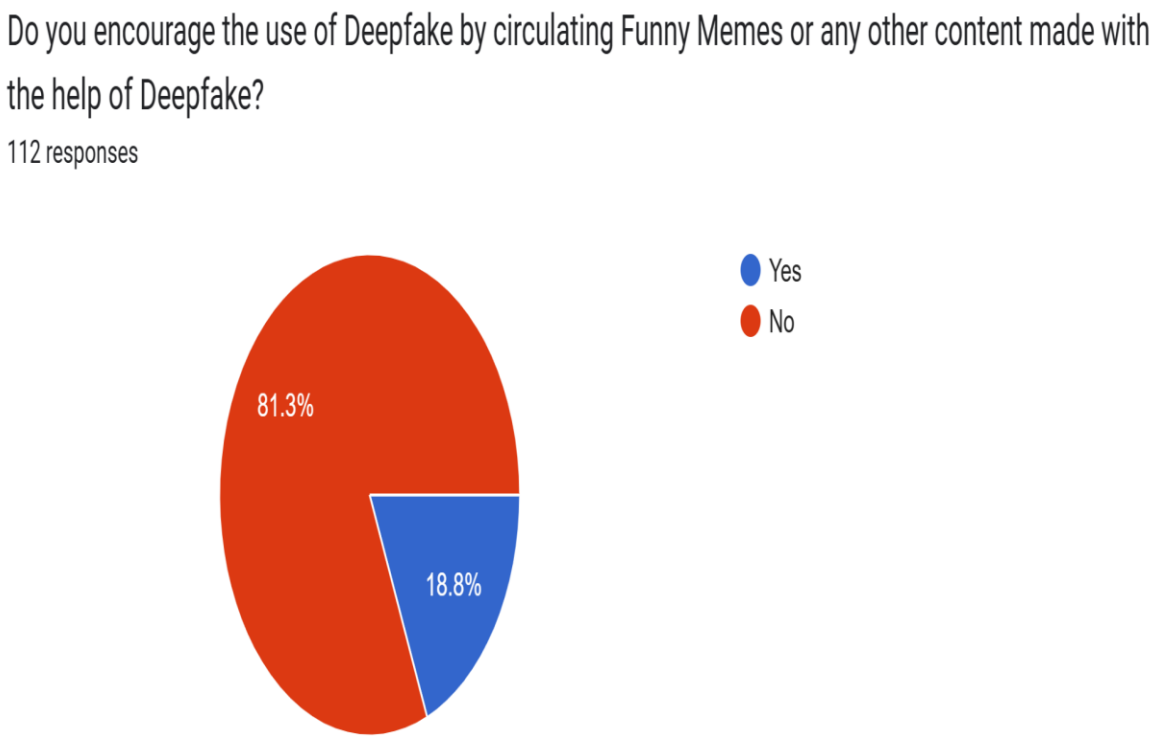
Therefore, the need arises that the intermediaries have an ethical and legal obligation to make sure that their platforms are not abused for the propagation of dangerous synthetic media.

The pie graphic makes it evident that most respondents believe intermediaries are important players in the spread of deep-fakes. Legally speaking, the results lend credence to calls for more robust intermediary regulation, better AI governance, and increased cyber law enforcement.
The graph also illustrates the increasing public awareness of the risks deep-fake technology poses to society and the law, as well as the critical role digital platforms play in either preventing or facilitating these damages.
P.T.O
15.Given below is the pie-chart showing responses collected from question number 15 of the survey.



From the above given chart we get to see that approximately 93.8% of the responses are believing that the spread of deep-fakes is mostly caused by social media platforms. While, 6.3% (No): A small percentage of respondents do not believe that social media plays a significant role in the spread of deep-fakes.

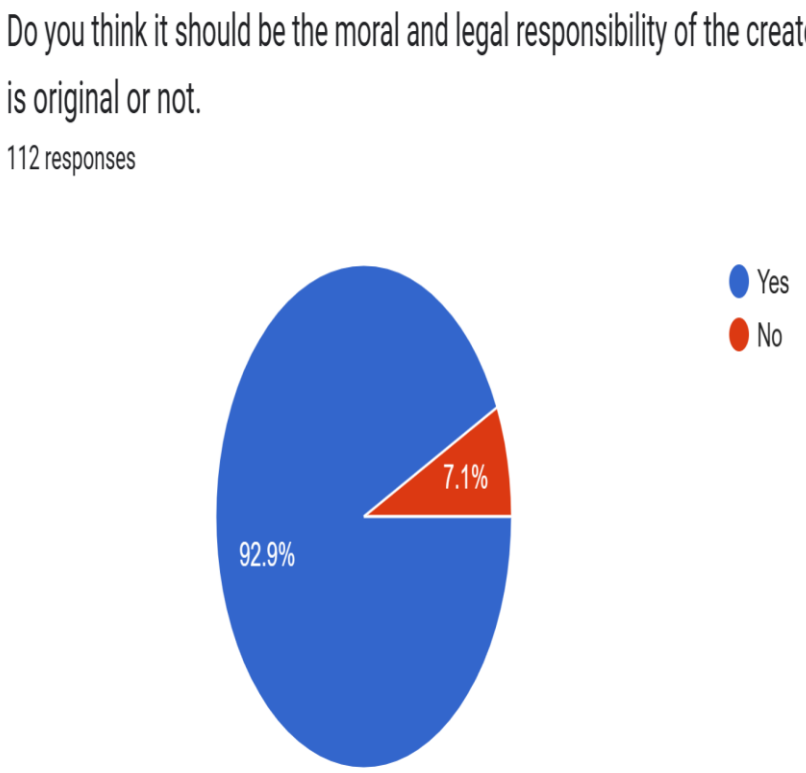
Nearly 94% of respondents mention social media, which speaks directly to the idea of safe harbour protection and reflects a growing public opinion that platforms are not doing enough.
Bad actors need a large collection of crisp images and audio in order to produce a high-quality deep-fake. People voluntarily post their biometric information (voices and faces) on social media, which is the main harvesting ground.
Engagement-driven algorithms are used by social media companies. Deep-fakes frequently go viral quickly because they are dramatic, contentious, or provocative.
The data clearly shows that the public sees deep-fakes as an epidemic actively fuelled by social media platforms distribution design rather than just as a limited technology problem.
P.T.O
16. Below is the pie-chart showing responses collected in the survey on question number 17



From, the above given chart we can conclude that approximately 81.3% responses are disagreeing that they don't share memes made with the help of deep-fake, while 18.8% are stating that they share deep-fake material like memes.
The vast majority of respondents (81.3%) who selected "No" indicate that people are extremely wary about deep-fake technology. From a legislative standpoint, this strong rejection gives politicians the authority to create more stringent regulations. It suggests that society believes the potential negative effects of deep-fakes such as false information, identity theft, and non-consensual synthetic media far exceed any funny or entertaining value.
Although 18.8% of respondents support deep-fakes for memes, this small percentage draws attention to a serious legal flaw. Defendants frequently invoke the "parody" or "satire" to protect in court to assert their right to free speech protections. But as a law student would point out, proving intent can be challenging. Regardless of the original goal, strong regulation is required because a deep-fake developed as a "funny meme" can be readily stripped of its context and exploited to libel a person, harm a reputation, or mislead the public.

The high "No" rate indicates that the majority of people are aware of the moral and possibly legal dangers of participating in the supply chain. Intermediaries (social media platforms) are under tremendous pressure, and nearly one-fifth of respondents are eager to post deep-fakes for light fun.

17.Given below is the pie-chart showing the responses collected on question number 18 of the survey.

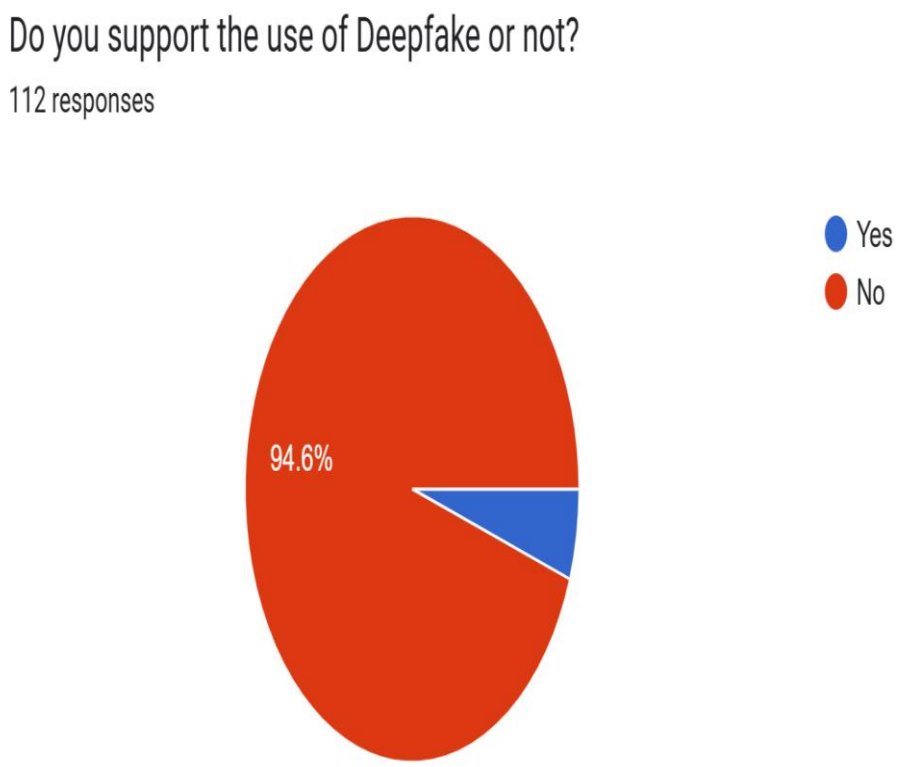


From the above given pie-chart we can conclude that 92.9% i.e. approximately 104 respondents believe that declaring content originality should be a moral and legal obligation for artists.

Also, 7.1% i.e. approximately 8 respondents don't think this should be a required duty of the creators.

The enormous public mandate for regulation is represented by the 92.9% majority. This suggests that the great majority of people now see content authenticity as a crucial issue requiring formal regulatory structures and enforcement methods rather than just a personal preference.
Transparency is strongly favoured by the people, according to the research. Legally speaking, this encourages the use of stringent "Right to know" and consumer protection regulations. If included into IP law, it would shift the burden of proof to the creator and mandate disclosures (such watermarking AI-generated media or clearly citing synthesized works) in order to stop fraud and false information.
Despite its small size, the 7.1% minority offers a significant legal counterargument. This group probably draws attention to the practical difficulties of such a statute from a defensive or regulatory standpoint. Mandatory originality claims could violate free expression, impose excessive administrative burdens on independent artists, and create significant jurisdictional obstacles in a global digital environment.
In the end, the graph shows that public opinion is strongly in favour of digital accountability. As a law student, this highlights the pressing necessity for legislators to create thorough transparency laws that safeguard intellectual integrity without impeding original thought.

18.Given Below Is The Responses Collected In The Survey On Question Number 19 Of The Survey:



From the pie-chart we can see that remarkably, 94.6% of respondents said they oppose the usage of deep-fakes. Legally speaking, this broad agreement shows a general public concern about the effects of synthetic media on privacy, individual rights, and systemic truth.

The use of deep-fakes is only supported by 5.4% of respondents. This tiny minority probably sees the technology through the prism of entertainment, artistic expression, or useful uses (such film or historical preservation), all of which are often protected by the right to free speech and expression.
The stark distinction explains why regulatory agencies are rushing to enact laws in this area. The 94.6% resistance is in line with the serious legal threats that deep-fakes provide, such as identity theft, defamation, the unlawful production of explicit content without consent, and the manipulation of democratic processes (such as election meddling).

OVERALL ANALYSIS OF THIS SURVEY:

The claim that deep-fake technology has already affected public opinion is supported by empirical data from the survey results. Despite the small sample size of 112 respondents, the results are still significant since they show a more general trend of doubting about digital originality. Discussions about AI governance, digital evidence standards, cyber law reform, and online privacy protections can all benefit from this data.
Additionally, the graphic recommends that organizations including governments, courts, academic institutions, and tech firms work together to create systems for confirming digital authenticity. Watermarking technology, AI detection systems, more stringent platform laws, and forensic analysis techniques for digital evidence are a few examples of this. To ascertain whether electronic content has been altered, legal systems might also require professional cyber forensic specialists.

In summary, the pie chart shows that the public's confidence in the authenticity and uniqueness of digital content has been greatly impacted by deep-fake technology. Critical legal issues pertaining to cybercrime, digital evidence, privacy,

defamation, constitutional rights, and AI legislation are highlighted in this survey data. The results highlight how urgently extensive legal reforms, public awareness campaigns, and technological protections are needed to confront the increasing problems that deep-fake technology presents to contemporary society.

This information gives legislators and legal scholars a compelling case for more stringent regulations. It indicates that specific, enforceable digital safety legislation and required watermarking of synthetic content are necessary since the public may perceive current tort laws and criminal statutes as inadequate to address the particular difficulties posed by AI-generated disinformation.

CHAPTER 5

CONCLUSION AND SUGGESTIONS:

As we have seen that how the deep-fake technology has evolved, also how the deep-fake technology is not limited only to the technological use only, it is creating an interlinking between various sectors like the fundamental right to privacy, data protection and the cyber security. We have examined, the evolution of deep-fakes, it's use in both positive manner as well as in malicious manner, it's social impact, the way it is affecting right to privacy and the intellectual property, we can conclude that the deep-fake is now have reached to a level where it has created a complex socio-legal challenge in the society. The deep-fake is violating the fundamental rights of the individuals as well as it is affecting the democratic institution of a country, digital trust of the social media platforms and cyber security.

We have also seen that how from using CGI [Computer generated imagery] to using GANs the AI developed. With the help of this the synthetic media are now being easily accepted by our society. As with the help of GAN technology it has become easy to generate hyper realistic audio, video, images etc. Earlier it was mainly used in the entertainment industry but now, the use of synthetic media is in education, medical profession, media etc. in very different fields.

Because of the deep-fake technology, the evidentiary value of the digital evidence is being altered and created legal concerns regarding the authenticity of the evidence produced. Deep-fakes is also causing problem in constitutional and ethical issues like the right to privacy and freedom of speech. The legislation must enact some kind of law by maintaining a balance between constitutional protection given to an individual and the technological advancement taking place. But also maintain the technological freedom for the further development of the technology, as if the rules will exceed it can affect adversely the development of AI technology. Also the lack of regulation will encourage the criminals to do financial frauds, sharing of non-consensual images and videos, at a larger extent it can be a threat to our national security also.

When we analyze the uses of deep-fake, we will get to know the dual nature of deep-fake technology i.e. the positive use of deep-fake and the malicious use of deep-fake. In positive manner, it is widely used in the entertainment industries, in the educational sector for teaching, healthcare services and also in businesses like e-commerce. And for malicious use it is used in generating and spreading deep-fake porn videos by grafting the face of the victim with the body of someone else, in the Phishing attacks, here the attacker can change his/her voice with the help of AI into the voice of the known person of the victim to get the desired financial transfer, Deep-fakes have the capacity to agitate the crowd and thus can cause the results of the elections can get hampered because of it etc. The rise in the AI generated disinformation, biometric spoofing etc. are creating a serious concern in the field of digital forensic system.

One of the most important steps taken towards the proactive AI governance is through the Regulatory Paradigm of 2026. It includes the Mandatory Labelling i.e.if the content is synthetic, a label must be visible on 10% of the display surface, it also includes, Identity Disclosure i.e. the platforms are now legally obligated to reveal or to identify of a deep-fake creator of the victim upon request and at last it includes the Loss of Safe Shelter security of the Intermediaries in which the platform (intermediary) may be sued as the "publisher" of the crime and lose their immunity under Section 79 of the IT Act if they do not delete a reported deep-fake within the allotted two to three hours of the provided timeline.

From legal perspective, we can say that the present legal system is struggling in dealing with the synthetic media like deep-fakes. There are a lot of loopholes present in the current laws regarding the new technologies related to AI. Also, when we look closely into the Indian legal system, we will find that it exhibits both the progress and the weakness regarding the threat posed by deep-fakes. Now, by looking into the legal provisions under the BNS 2023, IT Act 2000, Intellectual

property laws etc. are providing partial remedies for the crimes like online defamation, obscenity, digital fraud, impersonation and disinformation. Now, the remedies available for all the offenses mentioned under the IT Act can partially provide remedies for the crimes done with the help of AI. There is not a single defined legislature in the Indian Legal system that can provide remedy for the AI generated manipulations and synthetic media like Deep-fake. The responsibility among the users, intermediaries, government, middlemen is not specified properly which is creating a regulatory gap in the society regarding technologies like deep-fake.

The ability of the technology to undermine "truth" presents a systemic risk to the legal system, notwithstanding its enormous creative potential. The task is on the Indian legal system, as they will have to establish strong guidelines regarding the use of AI technology like deep-fakes. Also, they will have to create strong “Guardrails” against the misuse of the technology like the GANs.
Nowadays, synthetic media had become a powerful force that is changing the fact that how society views authenticity, truth, and identity. Every new skill offers significant advantages, but it also creates new opportunities for coercion, fraud, and misinformation.

In today’s digital word, where there is a significant use of AI is happening in various fields of life, then the organisations cannot depend on the manual human inspection or intuition for checking the authenticity of the material available.
Because deep-fakes undermine both individual rights and societal ideals, their social impact is especially concerning. Deep-fakes have the ability to sway public opinion, manipulate emotions, and cause widespread misunderstanding. These negative effects are greatly increased by the quick spread of altered content via social media platforms. People are vulnerable to social exclusion, cyberbullying, emotional distress, and reputational harm. Deep-fakes with political motivations have the potential to disrupt democratic institutions, inflame tensions within communities, and tamper with elections. Beyond immediate victims, the psychological effects of synthetic media add to a more general atmosphere of mistrust and worry.

The technology is growing at a very fast speed, in a very small duration of time, we often get to see some enhancement in the tech-world, thus, there is a need of such technology that can match the speed of the changing technology in terms of detecting the AI based materials.
There is a need of an automated detection system, which detects the use of AI technologies like deep-fake and aware the users about the use of AI in the material. In the year 2021, the Reality Defender was introduced whose work is to detect the deep-fake and to assist the government etc. for protecting the identity and trust of the individuals. Reality Defender is currently leading in the market of deep-fake detection which comes under the sector of cyber security, it is helpful for the institutions to stop the AI generated content before getting viral and before creating any kind of problematic situation.
Fake information is very easy to transmit, but it is way more difficult to stop the passing of those falsely generated deep-fake information, also it is very difficult to store and update the records regarding the deep-fake.
Victims' pain is made worse by the insufficiency of legal remedies in many jurisdictions. The peculiarity of AI-generated sexual content may not be sufficiently addressed by current obscenity and cybercrime regulations, particularly when no actual physical act took place. Procedural obstacles, delayed takedowns, insufficient law enforcement responses, and challenges in identifying anonymous attackers are commonplace for victims. As a result, the emergence of non-consensual deep-fake pornography highlights the critical need for victim-based legal frameworks and quick reaction times.

Deep-fakes' violation of people's right to privacy and dignity is a reflection of the larger conflict between the growth of technology and the protection of human rights. By using personal information without permission, deep-fakes compromise informational autonomy. By dehumanizing, objectifying, and misrepresenting people in made-up situations, they violate people's dignity.

Non-consensual deep-fake pornography, which disproportionately targets women and marginalized groups, exacerbates the issue. Such abuse is a type of digital sexual assault that has its roots in cyber sexism and patriarchal power structures. The severe psychological, emotional, and reputational harm that victims endure shows that digital violations can have just as much of an impact as physical ones.

Additionally, deep-fakes pose serious dangers for identity theft, impersonation, defamation, and violations of publicity rights. AI-generated media's realism increases reputational harm and makes fraud, deceit, and economic exploitation easier. Even though they are somewhat applicable, the current legal frameworks are still disjointed and insufficient to handle the complexity of the harms caused by synthetic media.

An essential moral basis for controlling deep-fakes is provided by constitutional rights pertaining to privacy, dignity, reputation, and autonomy. Legal protection is provided by judicial recognition of privacy under Article 21 and personality rights in Indian jurisprudence. But because AI technology is always changing, specific laws that can strike a balance between innovation and responsibility are needed.

Legal change, technology safeguards, platform responsibility, public awareness, and international cooperation are all necessary for an effective response to deep-fakes. Laws should ensure quick solutions for harmful information while taking a victim-focused and consent-based approach.

Deep-fake provide a profoundly human as well as technological issue. The idea that people must maintain control over their identity, appearance, and personal autonomy must be reaffirmed in order to defend privacy and dignity in the digital age. Legal systems must make sure that technology advancement does not compromise human dignity and constitutional liberties as artificial intelligence develops.

Deep-fakes present equally important intellectual property challenges. Large datasets with copyrighted photos, movies, audio files, books, and artistic items are usually used to train AI algorithms. There are concerns about whether using copyrighted content for AI training is acceptable fair use or infringement. A growing number of creators and copyright holders contend that their economic rights and creative labour are compromised by unapproved scraping and ingesting of their works.
However, developers argue that AI training entails transformational application, which is essential for technological growth and creativity. In many jurisdictions, the tension between innovation and copyright protection is still unresolved. In the context of machine learning, courts around the world are still debating issues related to consent, licensing, derivative works, and the limits of fair use.

The foundation of traditional copyright systems was identifiable acts of copying and human authorship. But generative AI makes it difficult to distinguish between imitation, replication, and inspiration. There are challenging issues with fair use, licensing, market substitution, and unapproved exploitation of creative labour when copyrighted works are included in AI training datasets. At the same time, deep-fake technologies put personality rights at risk by making it possible to digitally clone identities, voices, and faces without authorization.

Authorship and ownership are still unsolved issues. Lawmakers and courts around the world are still debating whether or not AI-generated works should be protected by copyright and who should be the owner of such rights. At the same time, artists, publishers, performers, and producers want more robust protections against unpaid exploitation.

At the heart of this argument is the fair use theory. While creators worry about economic displacement and the loss of artistic sovereignty, AI developers see fair usage as critical to technical advancement and machine learning research. Therefore, innovation must be balanced with justice, economic rights, consent, and human dignity in the legal system.

Future legal systems will probably need a mix of copyright reforms tailored to AI, mechanisms for licensing, the obligations for transparency, the protection for digital identities, International collaboration and the governance of ethical AI.
Intellectual property law must change as synthetic media develop in order to protect both technical advancement and the rights of human producers.

Countries all around the world are experimenting with various measures to deal with the threats posed by deep-fakes, according to a comparative examination of regulatory approaches. One of the most extensive initiatives to govern AI technologies using a risk-based framework is the European Union AI Act. The EU's commitment to striking a balance between innovation and the preservation of basic rights is demonstrated by its transparency duties, mandated labelling of synthetic content, accountability requirements, and stringent compliance standards.

The US takes a more dispersed strategy, relying on state-level legislation, sector-specific rules, and constitutional guarantees for free expression. While federal authorities concentrate on consumer protection and cyber-security issues, several states have passed legislation targeting deep-fakes and non-consensual pornography related to elections. However, extensive regulatory action is constrained by the constitution's significant emphasis on freedom of expression. Through legal initiatives like the Online Safety framework, the UK places a strong emphasis on harm reduction, platform accountability, and online safety. The UK strategy aims to maintain technological innovation while placing more accountability on digital platforms. These global experiences show that there isn't a one, widely recognized deep-fake regulation mechanism. However, recurring themes transparency, accountability, consent, platform duty, and user protection emerge.

In order to regulate synthetic media, social media platforms and intermediaries play a crucial role. Platforms have a major impact on the processes of detection, moderation, and removal because they serve as the main channels for the spread of deep-fakes. Frameworks for intermediary liability make an effort to strike a compromise between the necessity to prevent harm and the right to free speech. However, effective moderating is quite difficult due to the vast volume of internet content.

Automated detection techniques are still not perfect; they could produce false positives or miss complex modifications. Censorship, excessive removal of acceptable content, and limitations on political or artistic expression are other consequences of excessive regulation. As a result, platform governance needs to integrate technology solutions with human oversight, due process safeguards, transparency standards, and user awareness.

Despite increased exposure to modified content, empirical research on deep-fakes shows that public understanding of synthetic media is still low. Many people lack the technological literacy needed to recognize deep-fakes or comprehend their ramifications. Further research indicates that as AI systems advance, deep-fake detection gets harder. The public's confidence in digital information has decreased, especially among younger generations that primarily rely on social media for communication and news.

Additionally, empirical results show that women, prominent personalities, and marginalized communities are disproportionately vulnerable to deep-fake abuse. Inadequate institutional support, social isolation, and psychological trauma are common experiences for victims. Furthermore, scientists have stressed that the negative effects of synthetic media cannot be completely eradicated by technical fixes. Social responsibility, educational programs, legal reform, and ethical governance are all equally significant.

The whole analysis shows that deep-fake technology is a complex problem that calls for interdisciplinary solutions. Criminal legislation and content censorship are insufficient to confront technological advancement. Legal, technological, ethical, educational, and international aspects must all be integrated for effective governance. Both heavy regulation that hinders innovation and regulatory apathy that allows widespread misuse must be avoided by policymakers.

In the end, deeper conflicts in today's digital society are reflected in the emergence of deep-fakes. Humanity's creative potential has been enhanced by artificial intelligence, but it has also revealed flaws pertaining to truth, identity, privacy, and trust. Modern legal systems face the difficulty of developing frameworks that both uphold democratic norms, human dignity, and technological advancement in addition to punishing misuse.

The ability of society to create flexible legal frameworks, promote digital literacy, support ethical AI development, and advance global cooperation will determine how synthetic media regulation develops in the future. It is doubtful that deep-fake technology will go away. Rather, it will become more advanced, available, and incorporated into everyday life. Therefore, the goal should be responsible governance of the production, distribution, and use of synthetic media rather than their eradication.

To ensure that AI advances rather than undermines mankind, a balanced strategy based on human rights principles, innovation policy, constitutional values, and technological accountability is necessary. In the upcoming decades, the relationship between truth, technology, and democracy will be shaped by the legal and societal solutions that are implemented today.

SUGGESTIONS:

1. Adoption of a Comprehensive Law to Regulate Deep-fakes

The adoption of a comprehensive law that addresses deep-fake technology and synthetic media in particular is one of the most important recommendations.
The current legal framework, which includes information technology laws, criminal codes, copyright legislation, and privacy regulations, is disjointed and unable to handle the particular difficulties presented by AI-generated manipulation.

Deep-fakes, synthetic media, digital impersonation, and AI-generated manipulation should be all be precisely defined by a specific legal framework. Political propaganda, non-consensual pornography, identity fraud, financial frauds, and hostile impersonation are examples of damaging deep-fakes that must be classified by the law. To prevent uncertainty and guarantee efficient enforcement, precise definitions are crucial.
The proposed legislation ought to make a distinction between the legal and illegal applications of synthetic media. Within acceptable bounds, satire, parody, artistic expression, research, teaching, accessibility innovation, and entertainment should all be preserved. However, there should be severe legal and criminal sanctions for harmful applications that involve fraud, harassment, defamation, electoral meddling, or privacy abuses.
Procedural protections for victims, such as expedited complaint procedures, emergency takedown orders, compensation plans, and victim protection measures, should also be included in the legislation. The establishment of specialist digital courts or cyber tribunals could increase the effectiveness of adjudication.

2. Required Watermarking and Labelling of Synthetic Content

Governments ought to impose mandatory transparency requirements that mandate the watermarking or plain labelling of AI-generated information. Systems for identifying synthetic media can assist consumers in differentiating between real and fake-information.
AI generating systems should incorporate digital watermarking technologies from the outset. Investigators, platforms, and regulators can track down the source of modified the information with the help of these invisible indicators. Platforms that host synthetic content ought to make it clear to users that the content has been altered or created artificially.

3. Fortifying Consent and Privacy Frameworks

Individual liberty, consent, and dignity should be given top priority in deep-fake regulation. Except in specific legal exceptions like journalism, public interest reporting, satire, or law enforcement, no person's face, voice, likeness, or biometric data should be utilized to create synthetic media without informed consent.
Unauthorized digital cloning and biometric tampering should be specifically acknowledged as infringement of personality rights by privacy laws. Victims must be able to request the prompt removal of offensive content, financial compensation, injunctive remedy, and, if necessary, criminal prosecution.

4. Increased Protection against Deep-fake Pornography Without Consent

Governments must pass strict legislation that makes it illegal to produce, own, distribute, and publish non-consensual deep-fake pornography. Because they were not intended to deal with AI-generated sexual content, current regulations pertaining to obscenity and cybercrime are frequently insufficient.
Legal changes should guarantee that victims can prove injury without having to demonstrate actual physical exploitation. It should be illegal to create sexually explicit synthetic media.

Authorities should set up specific support systems, such as fast takedown units, legal help, counselling services, and assistance with digital forensics. Social media companies and search engines ought to be required by law to take down content that has been reported within a certain amount of time.
In order to give victims of online harassment and synthetic abuse a safer atmosphere, educational institutions and companies should also establish regulations addressing these issues.

5. Modification of Intellectual Property Laws for Content Created by AI

To handle AI-generated content and synthetic media, copyright law needs to be significantly changed. Legislators should specify which companies are entitled to ownership rights and make it clear whether AI-generated works are protected by copyright.
For the usage of copyrighted content in AI training datasets, explicit licensing procedures should be put in place. When their creations are used for machine learning, creators ought to be informed and, if necessary, paid fairly.

6. Fortifying the Liability Structure for Platforms and Intermediaries

In order to prevent dangerous deep-fake, social media companies, hosting companies, and middlemen must take the initiative. Platforms should be required by law to put in place appropriate methods for detection, reporting, moderation, and takedown.
Platforms should set up specific routes for reporting deep-fakes so that victims can request the quick removal of their content. Regular accountability reports and transparent moderating guidelines ought to be required.

7. Creation of Advanced Technologies for Deep-fake Detection

The creation of trustworthy deep-fake detection technology should get significant funding from governments, academic institutions, and private businesses. Reducing harm requires AI-based detection systems that can recognize altered voice, video, and images.
Innovation in forensic tools and authentication methods can be accelerated by public-private cooperation. Grants for the study of synthetic media dangers and detection techniques should be given to universities and research organizations.

8. Public awareness and digital literacy initiatives

Promoting media knowledge and digital literacy is one of the best long-term remedies to the deep-fake issue. The presence, dangers, and identification of synthetic media must be made clear to the public.
AI ethics, digital verification, cyber safety, misinformation, and media literacy should all be covered in school and university curricula. Pupils should be taught how to recognize manipulation tactics and critically assess online content.

Using digital channels, social media, public workshops, and television, governments and civil society organizations should launch national awareness campaigns. In order to properly report on AI-generated material and validate digital proof, journalists and media workers should undergo specific training.

9. International Collaboration and Standardization

It's because digital content often crosses national boundaries, deep-fake propagation is intrinsically international. Therefore, effective regulation and enforcement depend on international cooperation
To combat cross-border cybercrime and the misuse of synthetic media, nations should work together through treaties, mutual legal assistance agreements, and international organizations. Regulatory uniformity can be enhanced by common norms pertaining to openness, consent, labelling, and platform accountability.

10. Safeguarding electoral integrity and democratic processes

Elections, political debate, and democratic institutions are all seriously threatened by deep-fakes. Strict laws that forbid the malicious use of synthetic media during election campaigns should be implemented by governments. To detect and

eliminate dishonest political deep-fakes, election commissions and regulatory bodies should set up quick response systems. Mandatory disclosure laws should apply to political advertisements that use AI-generated content.

11.Acknowledgment of Digital Identity and Individual Rights

In the era of synthetic media, legal regimes ought to clearly acknowledge digital identity and personality rights. People must have legal control over how their voice, face, likeness, and biometric traits are used for commercial and technical purposes.

Unauthorized digital duplication and AI-generated cloning should be covered by an extension of the right to publicity. Celebrities, performers, influencers, and ordinary citizens alike should have remedies against unauthorized commercial exploitation of their identities.

In summary, deep-fake technology offers both tremendous potential and serious risk. Developing strong legal frameworks, moral protections, public awareness, and institutional resilience that can both protect society and promote responsible innovation is the way forward rather than opposing technological advancement. It is feasible to maximize the positive effects of synthetic media while reducing its negative effects on people, organizations, and democracy itself through responsible collective action and balanced governance.

BIBLIOGRAPHY:

1. https://www.researchgate.net/publication/398879751_The_Digital_Mirage_India's_Evolving_Legal_Battle_Against_Deepfake_Technology

2. https://www.researchgate.net/publication/391456796_DEEPFAKES_IN_INDIA_A_LEGAL_LABYRINTH_OF_COPYRIGHT_AND_IPR

3. https://academic.oup.com/ijlit/article-abstract/29/3/241/6409902?redirectedFrom=fulltext&login=false&utm_

4. https://timesofindia.indiatimes.com/india/shashi-tharoor-moves-delhi-high-court-to-block-ai-deepfakes/articleshow/130968876.cms

5. https://timesofindia.indiatimes.com/city/vijayawada/delhi-hc-restrains-ai-generated-film-exploiting-likeness-to-pawan-kalyans-son/articleshow/127725190.cms

6. https://www.researchgate.net/publication/401027453_Stolen_Faces_Borrowed_Voices_The_Legal_Imperative_for_Regulating_Deepfake_in_India

7. https://www.researchgate.net/publication/403662340_Intellectual_Property_and_Personal_Data_in_AI_Datasets_Under_India's_DPDP_Act_2023

8. https://www.theguardian.com/global-development/2025/nov/05/india-women-ai-deepfakes-internet-social-media-artificial-intelligence-nudify-extortion-abuse

9. https://lida.hse.ru/article/view/28690?utm_

10.https://arxiv.org/abs/2309.08133

11.https://www.reuters.com/legal/legalindustry/copyright-law-2025-courts-begin-draw-lines-around-ai-training-piracy-market-harm--pracin-2026-03-16/

12.https://www.reuters.com/legal/legalindustry/report-deepfakes-what-copyright-office-found-what-comes-next-ai-regulation-2024-12-18/

13.https://journals.ed.ac.uk/script-ed/article/view/12004?utm_

14.https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5153296

15.https://www.researchgate.net/publication/401027453_Stolen_Faces_Borrowed_Voices_The_Legal_Imperative_for_Regulating_Deepfake_in_India

16.https://journals.ed.ac.uk/script-ed/article/view/12004?utm_

17.https://zenodo.org/records/17606101
18.https://ijrlm.com/journal/legal-challenges-of-deepfake-and-synthetic-media-in-india/
19.https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5153296

20.https://academic.oup.com/ijlit/article-abstract/29/3/241/6409902?redirectedFrom=fulltext&login=false&utm_source

21.https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5532383

22.https://journals.ed.ac.uk/script-ed/article/view/12004?utm_

23.https://www.legalserviceindia.com/Legal-Articles/regulation-of-deepfakes-and-synthetic-media-legal-gaps-and-proposals/

24.https://www.leadindia.law/blog/en/are-deepfakes-illegal-in-india-and-what-are-the-penalties-in-2026/

25.https://lexfullegal.com/2025/12/30/deepfake-regulation-in-india-legal-challenges-solutions/

26.https://www.legalserviceindia.com/Legal-Articles/your-face-their-crime-a-legal-shield-against-deepfake-and-photo-harassment/

27.https://www.vifindia.org/article/2025/april/28/Bharatiya-Laws-Against-Deepfake-Cybercrime-Opportunities-and-Challenges

28.https://www.vifindia.org/article/2025/april/28/Bharatiya-Laws-Against-Deepfake-Cybercrime-Opportunities-and-Challenges

29.https://www.reddit.com/r/ClatReasoning/comments/1p13axu/deepfake_tech_law_legal_reasoning_new_question/?utm_https://www.clearlaw.online/articles/deepfake-regulation-in-india-the-3-hour-takedown-rule-constitutional-limits-and-the-urgent-case-for-a-dedicated-legal-framework

30.https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=2154268&utm_source=chatgpt.com&reg=3&lang=2

31.https://clt.nliu.ac.in/?p=1097

32.https://www.researchgate.net/publication/403632145_ARTIFICIAL_INTELLIGENCE_AND_CRIMINAL_LIABILITY_CHALLENGES_UNDER_THE_BHARATIYA_NYAYA_SANHITA_2023

33.https://timesofindia.indiatimes.com/india/ncw-recommends-legal-definition-penalties-under-criminal-law-to-counter-deep-fake-abuse/articleshow/125241763.cms

34.https://www.clearlaw.online/articles/deepfake-regulation-in-india-the-3-hour-takedown-rule-constitutional-limits-and-the-urgent-case-for-a-dedicated-legal-framework

35.https://www.legalserviceindia.com/Legal-Articles/deepfakes-and-the-law-a-growing-challenge-to-privacy-reputation-and-democracy/

36.https://journals.ed.ac.uk/script-ed/article/view/12004?utm_

37.https://www.legalserviceindia.com/Legal-Articles/your-face-their-crime-a-legal-shield-against-deepfake-and-photo-harassment/

38.https://www.researchgate.net/publication/385893846_Threat_of_deepfakes_to_the_criminal_justice_system_a_systematic_review

39.https://doi.org/10.1177/2372732218814855

40.https://doi.org/10.1145/3287763

41.https://doi.org/10.1016/j.procs.2018.07.279

42.https://doi.org/10.1145/3297722

43.https://doi.org/10.1007/978-3-030-20984-1_4

44.https://doi.org/10.1016/j.procs.2018.10.171

45.Coping with Grief and Loss: Stages of Grief and How to Heal

46.https://doi.org/10.1353/tj.2018.0097

47.https://doi.org/10.1016/j.procs.2017.11.106

48.https://doi.org/10.1016/j.intell.2017.10.005

49.https://doi.org/10.1109/MCSE.2018.2874117

50.https://doi.ieeecomputersociety.org/10.1109/MIS.2018.2877280

51.https://doi.org/10.1080/00963402.2019.1629574

52.https://doi.org/10.1016/j.chb.2017.11.034

53.https://doi.org/10.1109/ACCESS.2019.2905689

54.https://doi.org/10.1007/s00799-018-0261-y

55.https://doi.org/10.1515/opis-2019-0003

56.https://www.researchgate.net/publication/337644519_The_Emergence_of_Deepfake_Technology_A_Review

57.https://doi.org/10.1145/3309699

58.https://doi.org/10.1177/1365712718807226

59.https://doi.org/10.1007/s42438-018-0025-4

60.A Brief History of Deepfakes — Reality Defender
61.https://doi.org/10.1109/MITP.2019.2910503

62.https://techlawforum.nalsar.ac.in/web-2-0-solutions-for-web-3-0-problems-intermediary-liability-and-the-deepfake-crisis-in-india/#:~:text=To%20support%20this%2C%20the%20Draft,forfeit%20their%20Safe%20Harbour%20protection

63. https://www.vaishlaw.com/regulation-of-ai-generated-deepfake-content-and-synthetically-generated-information-sgi-in-india/

64.80% Of Surveyed Businesses Don't Have Plans For An AI-Related Crisis

65.https://primeinfoserv.com/blog-ai-deepfake-law-india-it-rules-2026-amendment/#:~:text=in%20India%2C%202026-,1.,Mandatory%20Warnings%20for%20AI%20Tools

66.https://pwonlyias.com/current-affairs/mandatory-labelling-of-ai-content-and-deepfake/

67.https://www.azbpartners.com/bank/88502/#:~:text=The%20Amendment%20Rules%20require%20intermediaries,and%20transmitting%20unlawful%20Synthetic%20Media%3B
68.https://www.insightsonindia.com/2026/02/11/it-rules-amendment-2026/#:~:text=Self%2DDisclosure%3A%20When%20you%20upload,video%20is%20actually%20a%20deepfake.
69.https://www.galaxyclasses.co.in/details?res_type=ca&res_id=9304#:~:text=Large%20platforms%20must%20deploy%20%E2%80%9Creasonable,and%20metadata%2Dbased%20authentication%20tools

70.https://www.aicerts.ai/news/it-rules-2026-indias-rapid-deepfake-crackdown/#:~:text=The%20Gazette%20demands%20prominent%20on,default%20features%20for%20Synthetic%20media
71.https://www.galaxyclasses.co.in/details?res_type=ca&res_id=9304#:~:text=Platforms%20with%20more%20than%205,is%20authentic%20or%20artificially%20created.

72.https://www.vaishlaw.com/regulation-of-ai-generated-deepfake-content-and-synthetically-generated-information-sgi-in-india/

73.https://www.vaishlaw.com/regulation-of-ai-generated-deepfake-content-and-synthetically-generated-information-sgi-in-india/

74.https://timesofindia.indiatimes.com/technology/tech-news/governments-new-it-rules-make-ai-content-labelling-mandatory-give-google-youtube-instagram-and-other-platforms-3-hours-for-takedowns/articleshow/128157496.cms#:~:text=Platforms%20must%20label%20all%20synthetically,modified%2C%20suppressed%20or%20stripped%20away.

75.https://www.azbpartners.com/bank/88502/#:~:text=Such%20Synthetic%20Media%20must%20be,identify%20that%20such%20information%20is

76.https://www.khaitanco.com/thought-leadership/MeitY-notifies-the-IT-Amendment-Rules-2026#:~:text=Labelling%20requirements%20for%20visual%20and,qualitative%20standard%20for%20permitted%20SGI

77.https://kankrishme.com/indias-2026-it-rules-amendment-regulating-ai-generated-content-and-accelerating-compliance/#:~:text=For%20particularly%20sensitive%20content%20(such,past%20delays%20in%20content%20moderation.%20

78.https://www.insightsonindia.com/2026/02/11/it-rules-amendment-2026/#:~:text=The%202026%20IT%20Rules%20amendment,of%20safety%20over%20safe%20harbour.

79.https://www.hoganlovells.com/en/publications/india-introduces-mandatory-labelling-for-ai-and-3hour-takedown-for-illegal-content#:~:text=To%20avoid%20sweeping%20in%20routine,that%20do%20not%20result%20in
80.https://visionias.in/blog/current-affairs/centre-notifies-it-rules-amendment-3-hour-takedown-deadline-for-ai-content#:~:text=The%20most%20transformative%20aspect%20of,%2C%20public%20order%2C%20or%20morality
81.https://www.livelaw.in/law-firms/law-firm-articles-/deepfakes-due-diligence-indias-2026-it-amendment-rules-resolve-global-platform-liability-debate-530344#:~:text=The%20amendment%20introduces%20%E2%80%9Csynthetically%20generated,clones%2C%20AI%2Dfabricated%20video

82.https://www.hoganlovells.com/en/publications/india-introduces-mandatory-labelling-for-ai-and-3hour-takedown-for-illegal-content#:~:text=SGI%20covers%20audio%2C%20visual%2C%20or,persons%20or%20real%E2%80%91world%20occurrences

83.https://skvlawoffices.com/indias-2026-amendment-to-it-rules-regulation-of-deepfakes-ai-content-and-the-three-hour-takedown regime/#:~:text=On%2010%20February%202026%2C%20the,the%20Information%20Technology%20Act%2C%202000

84.https://www.legal500.com/developments/thought-leadership/indias-new-it-rules-on-synthetic-media-a-comprehensive-legal-analysis/#:~:text=attract%20punishment%20under%3A-,Information%20Technology%20Act%2C%202000,Traffic%20(Prevention)%20Act%2C%201956

85.https://www.insightsonindia.com/2026/02/11/it-rules-amendment-2026/#:~:text=Section%2079%20Protection%3A%20Platforms%20generally,who%20created%20the%20illegal%20content

86.https://www.khuranaandkhurana.com/deepfake-regulation-india-2025-meity-s-comprehensive-it-rules-amendment#:~:text=Digital%20Personal%20Data%20Protection%20Act,violate%20fundamental%20DPDP%20Act%20principles

87.https://ledroitindia.in/the-legal-challenges-of-deepfakes-and-ai-ethics-in-the-indian-context/#:~:text=%E2%80%8BSection%20319%20(Cheating%20by,records%20(like%20deepfake%20evidence)
88.https://www.khuranaandkhurana.com/deepfake-regulation-india-2025-meity-s-comprehensive-it-rules-amendment#:~:text=For%20visual%20content%2C%20labels%20must,by%20intermediaries%20or%20end%20users
89.https://www.pib.gov.in/PressReleasePage.aspx?PRID=2154268#:~:text=Bharatiya%20Nyaya%20Sanhita%2C%202023%20(%E2%80%9C,cause%20public%20mischief%20or%20fear
90.https://www.insightsonindia.com/2026/02/11/it-rules-amendment-2026/#:~:text=The%202026%20IT%20Rules%20amendment,of%20safety%20over%20safe%20harbour

91.https://timesofindia.indiatimes.com/entertainment/hindi/bollywood/news/legal-implications-of-deepfake-image-like-that-of-rashmika-mandanna-and-katrina-kaif-usage-in-india/articleshow/105065690.cms#:~:text=Sections%2066E%20(Violation%20of%20privacy,The%20Indian%20Penal%20Code%20(IPC)

92.https://ledroitindia.in/the-legal-challenges-of-deepfakes-and-ai-ethics-in-the-indian-context/#:~:text=%E2%80%8BSection%2066D%20(Cheating%20by,like%20the%20corporate%20fraud%20cases

93.https://www.insightsonindia.com/2026/02/11/it-rules-amendment-2026/#:~:text=Digital%20Fingerprints%3A%20Platforms%20must%20embed,tool%20used%20to%20create%20it

94.https://recordoflaw.in/ai-and-deepfake-legal-challenges/#:~:text=More%20recently%2C%20in%202023%E2%80%9325,In%20Titan%20Ind

95.https://recordoflaw.in/regulation-of-deepfake-technology-can-existing-laws-cope/#:~:text=Abstract,from%20harassment%20to%20electoral%20manipulation

96.https://www.legal500.com/developments/thought-leadership/indias-new-it-rules-on-synthetic-media-a-comprehensive-legal-analysis/

97.https://www.insightsonindia.com/2026/02/11/it-rules-amendment-2026/

98.https://www.vintagelegalvl.com/post/the-synthetic-reality-assessing-india-s-regulatory-architecture-for-deepfakes#:~:text=Introduction,Generative%20Adversarial%20Network%20(GANs)

99.https://www.livelaw.in/mitigating-deepfake-threats-how-existing-laws-can-tackle-misuse#:~:text=This%20infringement%20of%20their%20personality,Simply%20Life%20India%20%26%20Ors

100. https://supremetoday.ai/indian-high-courts-weekly-cases-december-2025-to-january-2026-indian-high-courts-weekly-cases-december-2025-to-january-2026-20260105029#:~:text=Ashok%20Kumar%20(CS%20(COMM),5486)%2C%20where%20Advait%20M

101. https://journals.ed.ac.uk/script-ed/article/view/12004?utm_

102. https://law.shodhsagar.com/index.php/j/article/view/86?utm_

103. https://deepfake.co.in/awareness-education/the-legal-landscape-of-deepfakes-in-india-understanding-your-rights-and-remedies/?utm_

104. https://law.shodhsagar.com/index.php/j/article/view/86?utm_

105. https://www.indiacode.nic.in/handle/123456789/21433?utm_

106. https://www.indiacode.nic.in/handle/123456789/1999?utm_

107. https://www.indiacode.nic.in/handle/123456789/1999?locale=en&utm_

108. https://www.indiacode.nic.in/handle/123456789/15442?utm_

109. https://www.legalserviceindia.com/legal/article-15981-combating-deepfakes-with-inadequacies-of-existing-laws.html?utm_

110. https://arxiv.org/abs/2105.00192

111. https://arxiv.org/abs/2102.09603

112. https://arxiv.org/abs/2203.15044

113. https://en.wikipedia.org/wiki/Information_Technology_Act,_2000

114. https://www.wipo.int/wipolex/en/legislation/details/23164

115. https://arxiv.org/abs/2602.02754

116. https://www.mondaq.com/india/new-technology/1544224/deepfake-un-regulated-technology-its-menace-and-remedies

117. https://timesofindia.indiatimes.com/technology/tech-news/governments-new-it-rules-make-ai-content-labelling-mandatory-give-google-youtube-instagram-and-other-platforms-3-hours-for-takedowns/articleshow/128157496.cms

118. https://timesofindia.indiatimes.com/city/chandigarh/hc-notice-to-centre-others-on-plea-for-regulation-of-ai-generated-content/articleshow/129112789.cms

119. https://www.lawyersclubindia.com/articles/regulating-deepfakes-in-india-intermediary-liability-and-constitutional-limits--18208.asp

120. https://recordoflaw.in/deepfake-technology-and-criminal-law-is-india-prepared/

121. https://www.researchgate.net/publication/401027453_Stolen_Faces_Borrowed_Voices_The_Legal_Imperative_for_Regulating_Deepfake_in_India

122. https://www.researchgate.net/publication/398570892_Regulating_Artificial_Intelligence_in_India_Legal_Frameworks_Governance_Challenges_and_the_Path_Toward_a_Dedicated_AI_Law-_This_research_paper_authored_by_Ganesh_Shrirang_Satarkar_Nale_Department_of_S

123. https://www.ijllr.com/post/deepfakes-misinformation-the-indian-legal-vacuum-the-urgent-need-for-a-dedicated-deepfake-law

124. https://www.legalserviceindia.com/Legal-Articles/regulation-of-deepfakes-and-synthetic-media-legal-gaps-and-proposals/

125. https://www.ijllr.com/post/deepfakes-and-indian-criminal-law-addressing-the-gaps-in-legal-protection

126. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5153296

127. https://www.mondaq.com/india/new-technology/1544224/deepfake-un-regulated-technology-its-menace-and-remedies

128. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4411227

129. https://www.wipo.int/wipolex/en/legislation/details/23164

130. https://www.researchgate.net/publication/398879751_The_Digital_Mirage_India's_Evolving_Legal_Battle_Against_Deepfake_Technology

131. https://www.ijllr.com/post/deepfake-technology-and-cybercrime-a-critical-analysis-of-the-inadequacy-of-the-information-technol

132. https://www.tbalaw.in/post/india-s-it-intermediary-rules-2026-amendment-on-ai-generated-content-a-legal-analysis

133. https://ijlr.iledu.in/v6i88/

134. https://www.livelaw.in/mitigating-deepfake-threats-how-existing-laws-can-tackle-misuse#:~:text=This%20infringement%20of%20their%20personality,Simply%20Life%20India%20%26%20Ors

135. https://supremetoday.ai/indian-high-courts-weekly-cases-december-2025-to-january-2026-indian-high-courts-weekly-cases-december-2025-to-january-2026-20260105029#:~:text=Ashok%20Kumar%20(CS%20(COMM),5486)%2C%20where%20Advait%20M

136. https://www.legal500.com/developments/thought-leadership/indias-new-it-rules-on-synthetic-media-a-comprehensive-legal-analysis/

137. https://www.insightsonindia.com/2026/02/11/it-rules-amendment-2026/

138. https://www.vintagelegalvl.com/post/the-synthetic-reality-assessing-india-s-regulatory-architecture-for-deepfakes#:~:text=Introduction,Generative%20Adversarial%20Network%20(GANs)

139. https://recordoflaw.in/regulation-of-deepfake-technology-can-existing-laws-cope/#:~:text=Abstract,from%20harassment%20to%20electoral%20manipulation

140. https://www.insightsonindia.com/2026/02/11/it-rules-amendment-2026/#:~:text=Digital%20Fingerprints%3A%20Platforms%20must%20embed,tool%20used%20to%20create%20it

141. https://recordoflaw.in/ai-and-deepfake-legal-challenges/#:~:text=More%20recently%2C%20in%202023%E2%80%9325,In%20Titan%20Ind

142. https://timesofindia.indiatimes.com/entertainment/hindi/bollywood/news/legal-implications-of-deepfake-image-like-that-of-rashmika-mandanna-and-katrina-kaif-usage-in-india/articleshow/105065690.cms#:~:text=Sections%2066E%20(Violation%20of%20privacy,The%20Indian%20Penal%20Code%20(IPC)

143. https://ledroitindia.in/the-legal-challenges-of-deepfakes-and-ai-ethics-in-the-indian-context/#:~:text=%E2%80%8BSection%2066D%20(Cheating%20by,like%20the%20corporate%20fraud%20cases

144. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2154268#:~:text=Bharatiya%20Nyaya%20Sanhita%2C%202023%20(%E2%80%9C,cause%20public%20mischief%20or%20fear

145. https://www.insightsonindia.com/2026/02/11/it-rules-amendment-2026/#:~:text=The%202026%20IT%20Rules%20amendment,of%20safety%20over%20safe%20harbour

146. https://ledroitindia.in/the-legal-challenges-of-deepfakes-and-ai-ethics-in-the-indian-context/#:~:text=%E2%80%8BSection%20319%20(Cheating%20by,records%20(like%20deepfake%20evidence)

147. https://www.khuranaandkhurana.com/deepfake-regulation-india-2025-meity-s-comprehensive-it-rules-amendment#:~:text=For%20visual%20content%2C%20labels%20must,by%20intermediaries%20or%20end%20users

148. https://www.insightsonindia.com/2026/02/11/it-rules-amendment-2026/#:~:text=Section%2079%20Protection%3A%20Platforms%20generally,who%20created%20the%20illegal%20content

149. https://www.khuranaandkhurana.com/deepfake-regulation-india-2025-meity-s-comprehensive-it-rules-amendment#:~:text=Digital%20Personal%20Data%20Protection%20Act,violate%20fundamental%20DPDP%20Act%20principles

150. https://skvlawoffices.com/indias-2026-amendment-to-it-rules-regulation-of-deepfakes-ai-content-and-the-three-hour-takedown-regime/#:~:text=On%2010%20February%202026%2C%20the,the%20Information%20Technology%20Act%2C%202000

151. https://www.legal500.com/developments/thought-leadership/indias-new-it-rules-on-synthetic-media-a-comprehensive-legal-analysis/#:~:text=attract%20punishment%20under%3A-,Information%20Technology%20Act%2C%202000,Traffic%20(Prevention)%20Act%2C%201956

152. https://www.livelaw.in/law-firms/law-firm-articles-/deepfakes-due-diligence-indias-2026-it-amendment-rules-resolve-global-platform-liability-debate-530344#:~:text=The%20amendment%20introduces%20%E2%80%9Csynthetically%20generated,clones%2C%20AI%2Dfabricated%20video

153. https://www.hoganlovells.com/en/publications/india-introduces-mandatory-labelling-for-ai-and-3hour-takedown-for-illegal-content#:~:text=SGI%20covers%20audio%2C%20visual%2C%20or,persons%20or%20real%E2%80%91world%20occurrences

154. https://www.hoganlovells.com/en/publications/india-introduces-mandatory-labelling-for-ai-and-3hour-takedown-for-illegal-content#:~:text=To%20avoid%20sweeping%20in%20routine,that%20do%20not%20result%20in

155. https://visionias.in/blog/current-affairs/centre-notifies-it-rules-amendment-3-hour-takedown-deadline-for-ai-content#:~:text=The%20most%20transformative%20aspect%20of,%2C%20public%20order%2C%20or%20morality

156. https://kankrishme.com/indias-2026-it-rules-amendment-regulating-ai-generated-content-and-accelerating-compliance/#:~:text=For%20particularly%20sensitive%20content%20(such,past%20delays%20in%20content%20moderation.%20

157. https://www.insightsonindia.com/2026/02/11/it-rules-amendment-2026/#:~:text=The%202026%20IT%20Rules%20amendment,of%20safety%20over%20safe%20harbour

158. https://www.azbpartners.com/bank/88502/#:~:text=Such%20Synthetic%20Media%20must%20be,identify%20that%20such%20information%20is

159. https://www.khaitanco.com/thought-leadership/MeitY-notifies-the-IT-Amendment-Rules-2026#:~:text=Labelling%20requirements%20for%20visual%20and,qualitative%20standard%20for%20permitted%20SGI

160. https://www.vaishlaw.com/regulation-of-ai-generated-deepfake-content-and-synthetically-generated-information-sgi-in-india/

161. https://timesofindia.indiatimes.com/technology/tech-news/governments-new-it-rules-make-ai-content-labelling-mandatory-give-google-youtube-instagram-and-other-platforms-3-hours-for-takedowns/articleshow/128157496.cms#:~:text=Platforms%20must%20label%20all%20synthetically,modified%2C%20suppressed%20or%20stripped%20away

162. https://www.aicerts.ai/news/it-rules-2026-indias-rapid-deepfake-crackdown/#:~:text=The%20Gazette%20demands%20prominent%20on,default%20features%20for%20Synthetic%20media

163. https://www.galaxyclasses.co.in/details?res_type=ca&res_id=9304#:~:text=Platforms%20with%20more%20than%205,is%20authentic%20or%20artificially%20created

164. https://www.vaishlaw.com/regulation-of-ai-generated-deepfake-content-and-synthetically-generated-information-sgi-in-india/

165. https://www.insightsonindia.com/2026/02/11/it-rules-amendment-2026/#:~:text=Self%2DDisclosure%3A%20When%20you%20upload,video%20is%20actually%20a%20deepfake

166. https://www.galaxyclasses.co.in/details?res_type=ca&res_id=9304#:~:text=Large%20platforms%20must%20deploy%20%E2%80%9Creasonable,and%20metadata%2Dbased%20authentication%20tools

167. https://primeinfoserv.com/blog-ai-deepfake-law-india-it-rules-2026-amendment/#:~:text=in%20India%2C%202026-,1.,Mandatory%20Warnings%20for%20AI%20Tools

168. https://pwonlyias.com/current-affairs/mandatory-labelling-of-ai-content-and-deepfake/

169. https://www.azbpartners.com/bank/88502/#:~:text=The%20Amendment%20Rules%20require%20intermediaries,and%20transmitting%20unlawful%20Synthetic%20Media%3B

170. https://techlawforum.nalsar.ac.in/web-2-0-solutions-for-web-3-0-problems-intermediary-liability-and-the-deepfake-crisis-in-india/#:~:text=To%20support%20this%2C%20the%20Draft,forfeit%20their%20Safe%20Harbour%20protection

171. https://www.vaishlaw.com/regulation-of-ai-generated-deepfake-content-and-synthetically-generated-information-sgi-in-india/

172. 80% Of Surveyed Businesses Don’t Have Plans For An AI-Related Crisis

173. A Brief History of Deepfakes — Reality Defender

174. https://doi.org/10.1109/MITP.2019.2910503

175. https://doi.org/10.1515/opis-2019-0003

176. https://www.researchgate.net/publication/337644519_The_Emergence_of_Deepfake_Technology_A_Review

177. https://doi.org/10.1145/3309699

178. https://doi.org/10.1177/1365712718807226

179. https://doi.org/10.1007/s42438-018-0025-4

180. https://doi.org/10.1080/00963402.2019.1629574

181. https://doi.org/10.1016/j.chb.2017.11.034

182. https://doi.org/10.1109/ACCESS.2019.2905689

183. https://doi.org/10.1007/s00799-018-0261-y

184. https://doi.org/10.1353/tj.2018.0097

185. https://doi.org/10.1016/j.procs.2017.11.106

186. https://doi.org/10.1016/j.intell.2017.10.005

187. https://doi.org/10.1109/MCSE.2018.2874117

188. https://doi.ieeecomputersociety.org/10.1109/MIS.2018.2877280

189. https://doi.org/10.1177/2372732218814855

190. https://doi.org/10.1145/3287763

191. https://doi.org/10.1016/j.procs.2018.07.279

192. https://doi.org/10.1145/3297722

193. https://doi.org/10.1007/978-3-030-20984-1_4

194. https://doi.org/10.1016/j.procs.2018.10.171

195. Coping with Grief and Loss: Stages of Grief and How to Heal

196. https://www.asianinstituteofresearch.org/lhqrarchives/deepfake-technology-in-india-and-world%3A-foreboding-and-forbidding

197. https://www.researchgate.net/publication/401027453_Stolen_Faces_Borrowed_Voices_The_Legal_Imperative_for_Regulating_Deepfake_in_India

198. https://www.researchgate.net/publication/398570892_Regulating_Artificial_Intelligence_in_India_Legal_Frameworks_Governance_Challenges_and_the_Path_Toward_a_Dedicated_AI_Law-

199. https://academic.oup.com/ijlit/article-abstract/29/3/241/6409902?redirectedFrom=fulltext&login=false&utm_

200. https://journals.ed.ac.uk/script-ed/article/view/12004?utm_

201. https://or.niscpr.res.in/index.php/JIPR/article/view/17916?utm_

202. https://lida.hse.ru/article/view/28690?utm_

203. https://or.niscpr.res.in/index.php/JIPR/article/view/1205?utm_

204. https://lawjournals.celnet.in/index.php/jiprl/article/view/2004?utm_

205. https://www.reuters.com/sustainability/boards-policy-regulation/india-panel-review-copyright-law-amid-legal-challenges-openai-2025-05-06/

206. https://timesofindia.indiatimes.com/city/mumbai/truly-alarming-bombay-high-court-orders-removal-of-deepfake-content-infringing-akshay-kumars-personality-rights/articleshow/124611724.cms

207. https://timesofindia.indiatimes.com/legal/news/delhi-hc-bars-unauthorised-ai-deepfakes-using-yoga-guru-swami-ramdevs-persona-orders-platforms-to-take-down-content/articleshow/128771019.cms

208. https://www.reuters.com/sustainability/society-equity/spooked-by-ai-bollywood-stars-drag-google-into-fight-personality-rights-2025-10-01/

209. https://www.researchgate.net/publication/398879751_The_Digital_Mirage_India's_Evolving_Legal_Battle_Against_Deepfake_Technology

210. https://arxiv.org/abs/2402.09581

211. https://www.reuters.com/legal/legalindustry/report-deepfakes-what-copyright-office-found-what-comes-next-ai-regulation-2024-12-18/

212. https://arxiv.org/abs/2406.11857

213. https://lawjournals.celnet.in/index.php/jiprl/article/view/2004?utm_
214. https://iprtrends.com/TIPR/article/view/47?utm_

215. https://www.researchgate.net/publication/391456796_DEEPFAKES_IN_INDIA_A_LEGAL_LABYRINTH_OF_COPYRIGHT_AND_IPR

216. https://www.sciencedirect.com/org/science/article/abs/pii/S205346202500004X

217. https://iprtrends.com/TIPR/article/view/13?utm_

218. https://bpasjournals.com/library-science/index.php/journal/article/view/465?utm_

219. https://www.researchgate.net/publication/398879751_The_Digital_Mirage_India's_Evolving_Legal_Battle_Against_Deepfake_Technology
220. https://www.uscourts.gov/court-programs/bankruptcy/bankruptcy-basics/chapter-11-bankruptcy-basics

221. https://en.wikipedia.org/wiki/Digital_Personal_Data_Protection_Act,_2023

222. https://indiankanoon.org/doc/118912881/

223. https://lawfullegal.in/a-constitutional-analysis-of-deepfakes-free-speech-and-the-indian-legal-vacuum/

224. https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=2154268&utm_

225. https://chambers.com/articles/ai-and-deepfakes-navigating-the-digital-revolution-and-its-dark-side

226. https://lawfullegal.in/deepfakes-and-the-law-a-new-age-threat-to-democratic-integrity/

227. https://www.mondaq.com/india/it-and-internet/1745436/indias-new-it-rules-on-synthetic-media-a-comprehensive-legal-analysis

228. https://www.lawyersclubindia.com/articles/regulating-deepfakes-in-india-intermediary-liability-and-constitutional-limits--18208.asp

229. https://www.clearlaw.online/articles/deepfake-regulation-in-india-the-3-hour-takedown-rule-constitutional-limits-and-the-urgent-case-for-a-dedicated-legal-framework

230. https://lawfullegal.in/regulating-deepfake-technology-balancing-free-speech-privacy-and-national-security/

231. https://recordoflaw.in/deepfake-technology-and-criminal-law-is-india-prepared/

232. https://arxiv.org/abs/2301.07829

233. https://en.wikipedia.org/wiki/Freedom_of_expression_in_India

234. https://chambers.com/articles/ai-and-deepfakes-navigating-the-digital-revolution-and-its-dark-side

235. https://www.reddit.com/r/ClatReasoning/comments/1p13axu/deepfake_tech_law_legal_reasoning_new_question/?utm

236. https://www.lawandjusticewiki.org/wiki/Deepfakes?utm_

237. https://anantamias.com/it-intermediary-guidelines-and-digital-media-ethics-code-amendment-rules-2025/

238. https://www.reddit.com/user/InternetFreedomIn/comments/1r1wt8x/it_intermediary_amendment_rules_2026_contradict/?utm_

239. https://www.reddit.com/r/YT_Faceless/comments/1rjj4t9/indian_new_info_tech_rules_2026_and_impact_on/?utm_

240. https://ijrti.org/papers/IJRTI2511099.pdf?utm_

241. https://anantamias.com/it-intermediary-guidelines-and-digital-media-ethics-code-amendment-rules-2025/

242. https://thelawdaily.com/deepfake-regulation-india/

243. https://www.researchgate.net/publication/398879751_The_Digital_Mirage_India%27s_Evolving_Legal_Battle_Against_Deepfake_Technology?utm_

244. https://timesofindia.indiatimes.com/india/shashi-tharoor-moves-delhi-high-court-to

245. https://www.researchgate.net/publication/403662340_Intellectual_Property_and_Personal_Data_in_AI_Datasets_Under_India%27s_DPDP_Act_2023?utm_source=chatgt.com

246. https://timesofindia.indiatimes.com/city/vijayawada/delhi-hc-restrains-ai-generated-film-exploiting-likeness-to-pawan-kalyans-son/articleshow/127725190.cms?utm_

247. https://www.theguardian.com/global-development/2025/nov/05/india-women-ai-deepfakes-internet-social-media-artificial-intelligence-nudify-extortion

248. https://www.researchgate.net/publication/391456796_DEEPFAKES_IN_INDIA_A_LEGAL_LABYRINTH_OF_COPYRIGHT_AND_IPR?utm_

249. https://www.reuters.com/legal/legalindustry/copyright-law-2025-courts-begin-draw-lines-around-ai-training-piracy-market-harm--pracin-2026-03-/

250. https://lida.hse.ru/article/view/28690?utm_

251. https://www.reuters.com/legal/legalindustry/report-deepfakes-what-copyright-office/

252. https://indiankanoon.org/doc/149679501/?utm_

253. https://www.researchgate.net/publication/403632145_ARTIFICIAL_INTELLIGENCE_AND_CRIMINAL_LIABILITY_CHALLENGES_UNDER_THE_BHARATIYA_NYAYA_SANHITA_2023

254. https://en.wikipedia.org/wiki/Bharatiya_Nyaya_Sanhita,_2023

255. https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=2154268&utm_

256. https://timesofindia.indiatimes.com/india/ncw-recommends-legal-definition-penalties-under-criminal-law-to-counter-deep-fake-abuse/articleshow/125241763.cms

257. https://www.lawandjusticewiki.org/wiki/Deepfakes?utm_

258. https://www.aaptaxlaw.com/bns/337-bns-forgery-of-record-of-court-or-of-public-register-etc-337-bharatiya-nyaya-sanhita-2023.html

259. https://en.wikipedia.org/wiki/Bharatiya_Sakshya_Act,_2023

260. https://timesofindia.indiatimes.com/city/ahmedabad/toi-nfsu-hacked-2-0-spotted-a-deepfake-save-and-act-in-48-hours/articleshow/127808050.cms

261. https://lawsection.in/cyber-crimes-under-bharatiya-nyaya-sanhita-2023-bns/

262. https://www.indiacode.nic.in/handle/123456789/21420?locale=hi&utm_

263. https://www.indiacode.nic.in/handle/123456789/20062?view_type=browse&utm_

264. https://aapki-website.com/index.php?type=bnss

265. https://www.researchgate.net/publication/398819599_LEGAL_GAPS_IN_DEEPFAKE_MISUSE_STRENGTHENING_CYBERCRIME_CRIMINALIZATION

266. https://clt.nliu.ac.in/?p=1097

267. https://projects.itforchange.net/online-violence-gender-and-law-guide/module-2-typologies-of-online-gender-based-offenses-in-law/2-2-morphing-deepfakes/?utm_

268. https://thediplomat.com/2025/03/indias-growing-misinformation-crisis-a-threat-to-democracy/

269. https://vhil.stanford.edu/publications/social-interaction/social-impact-deepfakes

270. https://www.un.org/en/about-us/universal-declaration-of-human-rights

271. https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

272. https://www.unesco.org/en/artificial-intelligence/recommendation-ethics

273. https://www.un.org/en/ai-advisory-body

274. https://artificialintelligenceact.eu/

275. https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

276. https://www.congress.gov/crs-products

277. https://leginfo.legislature.ca.gov/?utm_

278. https://www.cac.gov.cn/?utm_

279. https://www.gov.uk/government/collections/online-safety-bill

280. https://www.meity.gov.in/content/information-technology-act-2000?utm_

281. https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf?utm_

282. https://www.scobserver.in/cases/justice-k-s-puttaswamy-v-union-of-india-background/?utm_

283. https://www.brookings.edu/

284. https://www.technologyreview.com/topic/artificial-intelligence/

285. https://cyber.fsi.stanford.edu/

286. https://www.weforum.org/topics/artificial-intelligence/?utm_

287. https://oecd.ai/en/dashboards/policy-initiatives/artificial-intelligence-act-ai-act-9517

288. https://www.unesco.org/en/artificial-intelligence/recommendation-ethics

289. https://www.oecd.org/en/topics/ai-principles.html

290. https://www.reuters.com/business/un-report-urges-stronger-measures-detect-ai-driven-deepfakes-2025-07-11/

291. https://www.techradar.com/pro/european-union-wants-to-ban-ai-created-images-and-video-in-official-messaging

292. https://www.reddit.com/r/ArtificialInteligence/comments/1rkfmb3/deepfakes_and_the_law/?utm_

293. https://www.reuters.com/business/europe-takes-first-step-banning-ai-generated-child-sexual-abuse-images-2026-03-13/

294. https://www.unesco.org/en/artificial-intelligence/recommendation-ethics

295. https://arensic.international/the-future-of-ai-regulation-global-policies-compliance-risk-management/

296. https://www.oecd.org/en/publications/governing-with-artificial-intelligence_795de142-en/full-report/enablers-guardrails-and-engagement-for-unlocking-trustworthy-ai_2f817983.html

297. https://www.oecd.org/en/publications/the-oecd-reinforcing-democracy-initiative_9543bcfb-en/full-report/component-8.html

298. https://www.oecd.org/en/publications/oecd-digital-economy-outlook-2024-volume-1_a1689dc5-en/full-report/component-5.html

299. https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-council-europe

300. https://www.oecd.org/en/publications/facts-not-fakes-tackling-disinformation-strengthening-information-integrity_d909ff7a-en/full-report/component-5.html

301. https://op.europa.eu/en/publication-detail/-/publication/bd90819e-9b6c-11ec-83e1-01aa75ed71a1?utm_

302. https://www.unesco.org/en/artificial-intelligence/recommendation-ethics

303. https://ai-ei.org/global-approaches-to-ai-regulation-a-comparative-guideline/

304. https://www.institut-fuer-menschenrechte.de/menschenrechtsschutz/datenbanken/datenbank-fuer-menschenrechte-und-behinderung/detail/iccpr-und-art-22-un-brk

305. https://www.cambridge.org/core/books/commentary-on-the-international-covenant-on-civil-and-political-rights/article-17-privacy-home-correspondence-honour-and-reputation/5C2A432BF74C4289A49281A9279DAE35

306. https://www.woventeaching.org/udhr/article-19

307. https://www.frontlinedefenders.org/en/right/freedom-expression

308. https://www.uu.nl/en/education/universal-declaration-of-human-rights-75-years/udhr-in-words-and-images/udhr-articles-1-30/article-19-freedom-of-expression

309. https://legalknowledgebase.com/what-is-the-article-17-right-to-privacy?utm_

310. https://www.researchgate.net/publication/388331619_UDHR_Article_-19

311. https://thelaw.institute/privacy-and-data-protection/global-privacy-protections-iccpr-international-conventions/

312. https://www.wnypeace.org/2021/12/19/article-19-freedom-of-opinion-and-expression/?utm_

313. https://humanrights.gov.au/resource-hub/by-resource-type/articles/rights-and-freedoms/freedom-interference-privacy-family-home-and-correspondence-or?utm_

314. https://www.claiminghumanrights.org/udhr_article_12.html?utm_

315. https://www.claiminghumanrights.org/udhr_article_19.html?L=1%29&utm_

316. https://www.institut-fuer-menschenrechte.de/menschenrechtsschutz/datenbanken/datenbank-fuer-menschenrechte-und-behinderung/detail/iccpr-und-art-22-un-brk

317. https://www.institut-fuer-menschenrechte.de/menschenrechtsschutz/datenbanken/datenbank-fuer-menschenrechte-und-behinderung/detail/aemr-und-art-22-un-brk

318. https://www.udhr.de/frn.html?utm_

319. https://www.woventeaching.org/udhr/article-12

320. https://www.frontlinedefenders.org/en/right/freedom-expression

321. https://www.uu.nl/en/education/universal-declaration-of-human-rights-75-years/udhr-in-words-and-images/udhr-articles-1-30/article-19-freedom-of-expression

322. https://humanrights.gov.au/resource-hub/by-resource-type/articles/rights-and-freedoms/freedom-interference-privacy-family-home-and-correspondence-or?utm_

323. https://cgfoetestsite.mystagingwebsite.com/laws/udhr-article-19/

324. https://digitalfreedomfund.org/digital-rights-are-human-rights/article-12-the-right-to-privacy/?utm_

325. https://www.derechos.org/ddhh/expresion/trata.html?utm_

326. https://cambodia.ohchr.org/en/civil-society-fund-freedoms/freedom-expression

327. https://www.patternsofpower.org/patterns/appendix1/

328. https://privacy-article12.org/?utm_

329. https://researchprofiles.ku.dk/en/publications/article-12-udhr-the-right-to-privacy-significance-and-contemporar/?utm_

330. https://www.ag.gov.au/rights-and-protections/human-rights-and-anti-discrimination/human-rights-scrutiny/public-sector-guidance-sheets/privacy-and-reputation

331. https://www.scribd.com/document/869830081/ICCPR-Easy-to-Read-Commentary-WEB

332. https://www.aph.gov.au/parliamentary_business/committees/senate/legal_and_constitutional_affairs/completed_inquiries/1999-02/privacy/report/c03?utm_

333. https://2covenants.ohchr.org/About-ICCPR.html?utm_

334. https://irf.in.ua/p/42?utm_

335. https://www.un.org/en/about-us/universal-declaration-of-human-rights

336. https://hrlibrary.law.umn.edu/edumat/hreduseries/tb1b/Section3/udhr.html?utm_

337. https://www.un.org/en/about-us/universal-declaration-of-human-rights

338. https://www.un.org/en/udhrbook/index.shtml

339. https://regulations.ai/regulations/RAI-US-NA-DAH5XXX-2023?utm_

340. https://www.spglobal.com/market-intelligence/en/news-insights/articles/2026/4/house-lawmakers-introduce-deepfake-bill-to-require-ai-content-labeling-101092610?utm_

341. https://regulations.ai/regulations/RAI-US-NA-COPIFXX-2025?utm_

342. https://www.ftc.gov/legal-library/browse/statutes/tools-address-known-exploitation-immobilizing-technological-deepfakes-websites-networks-act-take-it?utm_

343. https://www.gov.ca.gov/2024/09/19/governor-newsom-signs-bills-to-crack-down-on-sexually-explicit-deepfakes-require-ai-watermarking/?utm_

344. https://www.mintz.com/insights-center/viewpoints/2191/2024-02-29-proposed-ftc-rule-would-hold-ai-companies-liable?utm_

345. https://www.thomsonreuters.com/en-us/posts/government/deepfakes-federal-state-regulation/?utm_

346. https://www.ftc.gov?utm_

347. https://www.congress.gov?utm_

348. https://www.dhs.gov?utm_

349. https://pmc.ncbi.nlm.nih.gov/articles/PMC10879008/

350. https://intellectual-property-helpdesk.ec.europa.eu/news-events/news/deepfake-global-crisis-2024-08-28_en?utm_

351. https://link.springer.com/article/10.1186/s40163-024-00226-6?utm_

352. https://disputeresolution.cyrilamarchandblogs.com/2024/01/truth-or-illusion-criminal-liability-of-digital-intermediaries-in-the-age-of-deepfakes/?utm_

353. https://www.lawyersclubindia.com/articles/regulating-deepfakes-in-india-intermediary-liability-and-constitutional-limits--18208.asp?utm_

354. https://www.cambridge.org/core/books/defeating-disinformation/safe-harbor-and-content-moderation-regulation-in-india/F3CFF38410DE759B338D1ED6C519A559?utm_

355. https://journals.sagepub.com/doi/10.1177/14614448241253138?utm_

356. https://arxiv.org/abs/2402.09581?utm_

357. https://www.theguardian.com/global-development/2025/nov/05/india-women-ai-deepfakes-internet-social-media-artificial-intelligence-nudify-extortion-abuse?utm_

358. https://intellectual-property-helpdesk.ec.europa.eu/news-events/news/deepfake-global-crisis-2024-08-28_en?utm_

359. https://link.springer.com/article/10.1186/s40163-024-00226-6?utm_

360. https://www.lawyersclubindia.com/articles/regulating-deepfakes-in-india-intermediary-liability-and-constitutional-limits--18208.asp?utm_

361. https://arxiv.org/abs/2312.04431?utm_

362. https://chambers.com/articles/regulation-of-synthetic-media-in-india-legal-implications-of-the-2026-amendments-to-the-it-rules?utm_

363. https://www.theguardian.com/global-development/2025/nov/05/india-women-ai-deepfakes-internet-social-media-artificial-intelligence-nudify-extortion-abuse?utm_

364. https://disputeresolution.cyrilamarchandblogs.com/2024/01/truth-or-illusion-criminal-liability-of-digital-intermediaries-in-the-age-of-deepfakes/

365. https://www.reddit.com/r/ClatReasoning/comments/1p13axu/deepfake_tech_law_legal_reasoning_new_question/?utm_

366. https://arxiv.org/abs/2312.04431

367. https://chambers.com/articles/regulation-of-synthetic-media-in-india-legal-implications-of-the-2026-amendments-to-the-it-rules

368. https://www.tbalaw.in/post/india-s-it-intermediary-rules-2026-amendment-on-ai-generated-content-a-legal-analysis

369. https://www.tracelawpartners.com/post/regulating-deepfakes-in-india-understanding-the-draft-amendments-to-the-it-rules-and-their-implicat

370. https://lawarticle.in/the-digital-dilemma-regulating-deepfakes-and-ott-platforms-in-indias-legal-landscape/

371. https://thelegalquorum.com/deepfakes-and-law-addressing-the-legal-vacum-in-synthetic-media-regulation/

372. https://www.researchgate.net/publication/381302175_Combatting_Deep-fakes_in_India_-_An_Analysis_of_the_Evolving_Legal_Paradigm_and_Its_Challenges

373. https://journals.sagepub.com/doi/10.1177/14614448241253138

374. https://www.tbalaw.in/post/india-s-it-intermediary-rules-2026-amendment-on-ai-generated-content-a-legal-analysis

375. https://www.indiacode.nic.in/handle/123456789/1999?locale=en&utm_

376. https://www.wipo.int/wipolex/en/legislation/details/23164

377. https://lddashboard.legislative.gov.in/actsofparliamentfromtheyear/information-technology-act-2000?utm_

378. https://www.indiacode.nic.in/handle/123456789/20062?utm_

379. https://www.un.org/en/about-us/universal-declaration-of-human-rights

380. https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

381. https://www.eff.org/issues/privacy

382. https://www.brookings.edu/articles/deepfakes-and-the-emerging-challenge-for-privacy-democracy-and-national-security/?utm_

383. https://jolt.law.harvard.edu/digest/deep-fakes-a-looming-challenge-for-privacy-democracy-and-national-security?utm_

384. https://www.natlawreview.com/article/deepfake-technology-legal-challenges-and-implications?utm_

385. https://www.unwomen.org/en/articles/facts-and-figures/facts-and-figures-ending-violence-against-women

386. https://www.law.cornell.edu/wex/right_of_publicity?utm_

387. https://cyber.fsi.stanford.edu/io/news/deepfakes-and-disinformation?utm_

388. https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

389. https://www.indiacode.nic.in/handle/123456789/1999?locale=en&utm_

390. https://www.wipo.int/wipolex/en/legislation/details/23164

391. https://lddashboard.legislative.gov.in/actsofparliamentfromtheyear/information-technology-act-2000?utm_

392. https://www.researchgate.net/publication/347934344_Information_Technology_Act2000

393. https://lawmint.com/bare-acts/information-technology-act-2000-bare-act-pdf-download/

394. https://commons.wikimedia.org/wiki/File:Justice_K._S._Puttaswamy_(Retd.)_and_Anr_vs_Union_of_India_and_Ors_(Aadhaar_Judgement).pdf

395. https://en.wikisource.org/wiki/Index:Justice_K._S._Puttaswamy_(Retd.)_and_Anr_vs_Union_of_India_and_Ors_(Aadhaar_Judgement).pdf

396. https://pdf4pro.com/view/in-the-supreme-court-of-india-civil-original-2e7db6.html?utm_

397. https://commons.wikimedia.org/wiki/File:Section_377_-_Supreme_Court_of_India_-_WP(C)_NO._76_OF_2016_Judgement_06-Sep-2018.pdf

398. https://pdf4pro.com/view/in-the-supreme-court-of-india-civil-original-27b70a.html?utm_

399. https://lddashboard.legislative.gov.in/hi/actsofparliamentfromtheyear/information-technology-act-2000?utm_

400. https://www.cambridge.org/core/journals/american-journal-of-international-law/article/abs/justice-ks-puttaswamy-retd-and-anr-v-union-of-india-and-ors/ED631B8F922039BEC5400086C8E34338

401. https://www.supremecourtcases.com/justice-k-s-puttaswamy-retd-and-anr-v-union-of-india-and-ors-3/?utm_

402. https://www.ebcwebstore.com/login.php?service=scc

403. https://natlex.ilo.org/dyn/natlex2/r/natlex/fe/details?p3_isn=110155&utm_

404. https://ddd.gov.in/document/information-technology-act-2000/

405. https://legislative.assam.gov.in/

406. https://www.sci.gov.in/?utm_

407. https://main.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf?utm_

408. https://journals.sagepub.com/doi/10.1177/14614448241253138

409. https://journals.ed.ac.uk/script-ed/article/view/12004?utm_

410. https://www.reuters.com/legal/legalindustry/report-deepfakes-what-copyright-office-found-what-comes-next-ai-regulation-2024-12-18/

411. https://arxiv.org/abs/2109.02874

412. https://link.springer.com/article/10.1007/s40319-025-01582-9

413. https://arxiv.org/abs/2502.15858

414. https://scholarlycommons.law.northwestern.edu/njtip/vol22/iss1/4/?utm_

415. https://journals.sagepub.com/doi/10.1177/27523543241289108

416. https://arxiv.org/abs/2102.06109

417. https://academic.oup.com/ijlit/article-abstract/29/3/241/6409902?redirectedFrom=fulltext&login=false&utm_

418. https://www.reddit.com/r/aiwars/comments/1rr1jqn/fairuse_training_overfitting_and_the_end_of/?utm_

419. https://www.reuters.com/legal/legalindustry/copyright-law-2025-courts-begin-draw-lines-around-ai-training-piracy-market-harm--pracin-2026-03-16/

420. https://www.reuters.com/legal/legalindustry/newsrooms-vs-neural-nets-how-courts-are-handling-dmca-claims-against-genai-2025-08-27/

421. https://digitalcommons.law.uw.edu/wjlta/vol19/iss1/1/?utm_

422. https://www.reddit.com/r/aiwars/comments/1krv7jn/association_of_research_libraries_training/?utm_

423. https://www.reddit.com/r/COPYRIGHT/comments/1ljh7ev/the_downloaded_pirated_copies_used_to_build_a/?utm_

424. https://www.ft.com/content/e2fa34b2-6987-494d-a81a-1bdb6693671f?syn-25a6b1a6=1

425. https://www.researchgate.net/publication/401027453_Stolen_Faces_Borrowed_Voices_The_Legal_Imperative_for_Regulating_Deepfake_in_India

426. https://journals.ed.ac.uk/script-ed/article/view/12004?utm_

427. https://lida.hse.ru/article/view/28690?utm_

428. https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/infringing-ai-liability-for-aigenerated-outputs-under-international-eu-and-uk-copyright-law/C568C6B717E9CFC45FB52E58E54B6BEC

429. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4630085

430. https://www.researchgate.net/publication/398879751_The_Digital_Mirage_India%27s_Evolving_Legal_Battle_Against_Deepfake_Technology?utm_

431. https://link.springer.com/article/10.1007/s40319-025-01582-9?utm_

432. https://journals.sagepub.com/doi/10.1177/14614448241253138?utm_

433. https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/infringing-ai-liability-for-aigenerated-outputs-under-international-eu-and-uk-copyright-law/C568C6B717E9CFC45FB52E58E54B6BEC?utm_

434. https://academic.oup.com/ijlit/article/29/3/241/6409902?rss=1&utm_

435. https://journals.ed.ac.uk/script-ed/article/view/12004?utm_

436. https://journals.sagepub.com/doi/10.1177/27523543241289108?utm_

437. https://digitalcommons.law.uw.edu/wjlta/vol19/iss1/1/?utm_

438. https://scholarlycommons.law.northwestern.edu/njtip/vol22/iss1/4/?utm_

439. https://www.reuters.com/legal/legalindustry/copyright-law-2025-courts-begin-draw-lines-around-ai-training-piracy-market-harm--pracin-2026-03-16/?utm_

440. https://www.reuters.com/legal/legalindustry/report-deepfakes-what-copyright-office-found-what-comes-next-ai-regulation-2024-12-18/?utm_

441. https://journals.sagepub.com/doi/10.1177/14614448241253138?utm_

442. https://link.springer.com/article/10.1007/s40319-025-01582-9?utm_

443. https://journals.sagepub.com/doi/10.1177/27523543241289108?utm_

444. https://arxiv.org/abs/2102.06109?utm_

445. https://www.reuters.com/legal/legalindustry/report-deepfakes-what-copyright-office-found-what-comes-next-ai-regulation-2024-12-18/?utm_

446. https://academic.oup.com/ijlit/article/29/3/241/6409902?rss=1&utm_

447. https://arxiv.org/abs/2502.15858?utm_

448. https://www.reuters.com/legal/legalindustry/copyright-law-2025-courts-begin-draw-lines-around-ai-training-piracy-market-harm--pracin-2026-03-16/?utm_

449. https://digitalcommons.law.uw.edu/wjlta/vol19/iss1/1/?utm_

450. https://scholarlycommons.law.northwestern.edu/njtip/vol22/iss1/4/?utm_

451. https://www.reddit.com/r/aiwars/comments/1krv7jn?utm_

452. https://www.ft.com/content/e2fa34b2-6987-494d-a81a-1bdb6693671f?utm_