IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, June 2025
Impact Factor: 7.67

# An Analysis of Legal Gaps and Enforcement Challenges in Addressing AI-Generated Deepfake Sexual Offences in India

**Narmadha. L**
B.A, LLB(Hons)
Saveetha School of Law, Saveetha Institute of Medical and Technical Sciences (SIMATS), Chennai
narmadhaloganathan5@gmail.com

**Abstract**: *Deepfake technology facilitated by artificial intelligence has evolved quickly, raising stern ethical, lawful, and law enforcement concerns. Deepfake technology, while usable for a whole range of justifiable purposes, is being illegally used to generate sexually explicit unwilling content. It is a critical analysis of the expanding threat of AI-driven deepfakes sexual crime in India through loopholes available in the legal framework and its enforcement problems. The study talks about the inadequacies of existing laws such as the Information Technology Act, 2000, the Indian Penal Code, 1860. The study* ***focuses*** *on critically examining the emergence of deepfake AI-based sexual offenses in India, the loopholes in the prevailing legal framework, and the law enforcement challenges arising out of these offenses.The research method adopted here is* ***Empirical research****. The sampling technique was conducted in a convenience sampling technique and the research sample size is 200 samples. The statistical tools employed are Clustered Bar Graphs. The key* ***findings*** *are Law enforcement agencies are hampered by the challenge of attributing and prosecuting deepfake creators due to the advancement of the technology and the lack of clear legal definitions. The study* ***concludes*** *that India has to adopt an all-around legal and technological plan to combat sexual crimes enabled through deepfakes effectively, ensuring better protection to the victims as well as tougher deterrence policies.*

**Keywords:** Sexual offences, Cyber offences , Deepfake technology, AI, Privacy

## I. INTRODUCTION

The rapid advancement of **artificial intelligence** (AI) technologies has revolutionized digital content creation, but it has also given rise to alarming misuse, most notably through deepfake technology. Deepfakes—hyper-realistic synthetic media generated by AI—pose a significant threat when used to create non-consensual sexual content, leading to severe psychological, reputational, and legal harm to victims. This primary aim of the study is to analyze the loopholes in laws, enforcement issues, and the relative efficacy of laws in India and the United States, in addition to considering the drivers behind deepfake-enabled sexual offenses and emerging trends in AI-based exploitation. The **objectives** of the study are to examine the challenges in prosecuting AI generated deepfake sexual offences and analyse the steps that could be taken to enhance the enforcement capabilities against deepfake sexual offences.

**Evolution:** The origins of deepfake technology can be traced back to 2014, when Ian Goodfellow introduced Generative Adversarial Networks (GANs), a groundbreaking development that enabled the creation of highly realistic synthetic media. Initially, deepfakes found legitimate use in fields such as entertainment, video games, and cinema—particularly in computer-generated imagery (CGI) and voice dubbing. **Government Initiative:** India does not have any specific law criminalizing deepfake-created sexual offenses at present. The Information Technology (IT) Act, 2000, that regulates cybercrimes, only punishes the transmission and publication of obscene material under Section 67 and 67A, but not specifically AI-created media. Apart from that, Sections 292 of the Indian Penal Code (IPC), 354A, 509, and 66E of the Information Technology Act do offer some relief from online sexual harassment and breach of privacy but were not specifically drafted to counter deepfake-based crimes. **Factors affecting :** Affordable Access to AI Tools:


DOI: 10.48175/IJARSCT-27634

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, June 2025
Impact Factor: 7.67

Easy access to the open-source deepfake tools has made it simple for cybercrime perpetrators to make non-consensual deep fake porn with little technical knowledge. Lack of Legal Deterrence: The lack of firm laws and provisions for enforcement enables the perpetrators to function with impunity. Social Stigma and Victim Silence: Victims, especially women, are reluctant to report sexual offenses based on deep fakes because of social shame, ignorance, and ineffectual legal remedy. Inadequate **Current trends:** There has been a quick escalation of deepfake-based cybercrimes in recent trends, where AI-powered sexual content is exploited for blackmail, revenge porn, extortion, and political defamation. Voice deepfakes have also made it possible for cybercriminals to hack audio recordings for sexual exploitation and impersonation scams. As AI models improve, deep fake detection tools lag behind, allowing perpetrators to go undetected more easily. Additionally, the sale of deep fakes on the dark web has also contributed to the proliferation of sexual crimes produced by AI. **Comparison:** India and the U.S. present striking contrasts in addressing deep fake-facilitated sexual crimes. While the U.S. has legislated specifically on deep fakes, India continues to bank on old cyber laws that are not specifically aimed at AI-created content.

**Objectives of the study:**

- To examine the challenges in prosecuting AI generated deep fake sexual offences.
- To analyse the steps that could be taken to enhance the enforcement capabilities against deepfake sexual offences.
- To understand the current legal framework is adequate enough to deals with the offences regarding AI related deepfake sexual offences.

## II. REVIEW OF LITERATURE

**Singh and Mehta (2019)** examined the legal framework in India concerning deepfake pornography and identified significant gaps in existing legislation. Using doctrinal research methodology and case analysis, they evaluated the Information Technology Act's applicability to deepfakes. The study found that while Section 67 and 67A of the IT Act address obscene and sexually explicit content, they fail to specifically address the unique harm of deepfakes where a person's likeness is used without consent. The researchers concluded that Indian legislation requires amendments to explicitly criminalize deepfake sexual content, recommending the creation of specific provisions that recognize the distinct harms of identity appropriation through AI technologies and suggesting implementation of both civil and criminal remedies for victims. **Gupta (2020)** investigated the challenges in prosecuting creators of AI-generated sexual deepfakes under Indian criminal law. Through comparative legal analysis across multiple jurisdictions and interviews with legal practitioners, the research explored the applicability of IPC sections related to defamation, obscenity, and privacy violations. The findings revealed significant evidentiary challenges in establishing criminal intent and identifying perpetrators in the digital environment, particularly when content crosses international boundaries. The study concluded that current criminal procedures are inadequate for handling sophisticated technological offenses, recommending specialized cybercrime units with AI expertise and suggesting international cooperation frameworks to address cross-border perpetration of deepfake crimes. **Sharma and Reddy (2020)** assessed the effectiveness of content moderation policies on social media platforms in preventing the circulation of deep fake sexual content in India. Employing mixed methods including platform policy analysis, content monitoring, and focus group discussions with platform users, the researchers evaluated response times and removal rates across major platforms operating in India. Their findings indicated inconsistent enforcement of platform policies, with significant delays in content removal particularly for non-celebrity victims. The study concluded that self-regulation by platforms was insufficient for protecting Indian users, recommending mandatory reporting requirements, standardized response protocols, and collaborative approaches between platforms and law enforcement to improve detection and takedown of harmful deep fake content. **Patel et al. (2021)** examined the psychological and reputational impact of deepfake victimization through a survey of 300 Indian women and case studies of 15 victims. The research employed in-depth interviews, trauma assessment scales, and social media impact analysis to evaluate both immediate and long-term consequences of deepfake victimization. Results showed significant psychological trauma including anxiety, depression, and suicidal

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, June 2025
Impact Factor: 7.67

ideation among victims, with particularly severe impacts in conservative communities where victims faced social ostracism. The authors concluded that existing legal remedies failed to address the rehabilitation needs of victims, recommending comprehensive victim support services including psychological counseling, reputation management assistance, and expedited non-public legal proceedings to prevent secondary victimization. **Kumar and Joshi (2021)** analyzed the jurisdictional challenges in prosecuting deep fake sexual offenses in India's federal structure. Using legal analysis and interviews with law enforcement officials across five states, they documented inconsistencies in interpretation and application of relevant laws. The study found significant variations in police responsiveness, technical capabilities, and court approaches to digital evidence across different states, creating a fragmented enforcement landscape. The researchers concluded that this inconsistency created enforcement gaps exploited by perpetrators, recommending standardized national protocols for handling deepfake complaints, centralized technical assistance for state police, and uniform judicial guidelines for evaluating digital evidence in deepfake cases. **Banerjee (2022)** investigated the technical challenges in detecting and attributing AI-generated deep fake content for legal proceedings in India. Through technical experiments, forensic analysis, and interviews with cybercrime investigators, the research assessed the capabilities of Indian law enforcement to identify sophisticated deep fakes. Findings revealed significant technical limitations in the Indian legal system, with most forensic laboratories lacking advanced AI detection tools and trained personnel. The study concluded that the rapidly evolving nature of deepfake technology was outpacing forensic capabilities, recommending public-private partnerships for developing detection technologies, specialized training for judicial officers, and the establishment of technological standards for digital evidence admissibility in deepfake cases. **Chopra and Sen (2022)** evaluated the adequacy of privacy laws in addressing the non-consensual use of personal images in deepfake generation in India. Through legal analysis of the Personal Data Protection Bill and comparative study with GDPR provisions, they examined how "image rights" are conceptualized in Indian jurisprudence. The research found that the proposed data protection framework focused primarily on data security rather than dignity and autonomy concerns central to deepfake victimization. The authors concluded that India's nascent privacy regime required specific right to image provisions, recommending explicit recognition of likeness and voice as protected personal attributes, mandatory deepfake detection disclosure requirements, and remedial mechanisms focused on rapid content removal and de-indexing from search engines. **Verma and Chaudhary (2023)** examined the intersection of freedom of expression and deepfake regulation through constitutional analysis and stakeholder interviews with legal experts, content creators, and platform representatives. Using a rights-balancing framework, they evaluated potential regulatory approaches against constitutional protections. Findings revealed complex tensions between protecting victims and avoiding overbroad restrictions that would chill legitimate creative expression. The study concluded that narrowly tailored regulations focusing on demonstrable harm rather than content-based restrictions would best withstand constitutional scrutiny, recommending "least restrictive means" approaches such as mandatory labeling requirements, platform accountability for known deep fakes, and remedies proportionate to actual rather than potential harm. **Mishra et al. (2023)** conducted a comprehensive gap analysis of Indian legal frameworks applicable to deepfake sexual offenses through systematic review of legislation, case law, and enforcement practices. Employing legal research methodology supplemented by interviews with 45 stakeholders including legislators, judges, and victims' rights advocates, they mapped areas of legal incoherence and inadequacy. **Das and Agarwal (2024)** explored community-based interventions and alternative justice mechanisms for addressing deepfake sexual violence in India, particularly in rural and semi-urban settings with limited access to formal legal systems. Through field research across three states including interviews, focus groups, and action research with local governance bodies, they documented existing informal resolution practices and their effectiveness. The study found that while formal legal remedies remained inaccessible to many victims, community interventions often reinforced patriarchal norms rather than supporting victims. **Sharma and Banerjee (2023)** investigated the adequacy of existing Indian privacy frameworks in addressing deepfake harms through a comprehensive legal analysis of the Personal Data Protection Bill, Information Technology Act, and relevant case law, complemented by expert interviews with 28 privacy advocates, technologists, and legal scholars. Their aim was to identify specific privacy principles and provisions that could be leveraged or expanded to address deepfake sexual content. **Kumar and Sen (2024)** examined the cross-jurisdictional challenges in regulating deepfake technology through comparative legal analysis of 15

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, June 2025
Impact Factor: 7.67

international approaches and 35 expert interviews with legal practitioners, technologists, and policy experts across multiple countries. Their research aimed to develop recommendations for an Indian legal framework that could address the inherently global nature of deepfake creation and distribution. **Patel and Deshmukh (2024)** conducted an interdisciplinary study examining technical attribution challenges in deepfake investigations through experimental research involving the creation and forensic analysis of 200 deepfake videos using various AI techniques. Their research aimed to develop practical investigative methodologies specifically for Indian law enforcement contexts with limited technical resources. **Singh and Kapoor (2024)** analyzed the implications of emerging "voice deepfake" technology in the Indian context through case studies of 30 reported incidents and technical analysis of current voice synthesis capabilities. Their research aimed to assess whether existing legal frameworks addressing visual deepfakes could adequately extend to audio impersonation.. **Mishra et al. (2024)** explored the intersection of deepfake technology and traditional defamation law through doctrinal legal research examining 45 Indian court judgments involving digital defamation, complemented by comparative analysis of international approaches. Their aim was to assess whether traditional reputation protection mechanisms could effectively address deepfake harms. Findings revealed significant evidentiary challenges unique to deepfakes, with courts struggling to apply traditional defamation standards of "publication," "falsehood," and "reputational harm" to synthetically generated content. The researchers concluded that while defamation law offered some remedial pathways, especially regarding damages, **Iyer and Malhotra (2024)** conducted action research in collaboration with three major social media platforms operating in India, developing and testing algorithmic detection systems specifically calibrated for Indian contexts. The researchers concluded that effective regulation required both legal mandates and technical standards for platform implementation, recommending that India's forthcoming Digital India Act include specific provisions requiring platforms to implement detection technologies with minimum accuracy thresholds for Indian contexts. **Chatterjee and Pillai (2024)** examined the potential of non-legal interventions in addressing deepfake harms through educational research involving pre-post assessment of 3,000 secondary school students across 45 Indian schools who participated in digital literacy programs. Their study aimed to evaluate whether preventive education could effectively complement legal approaches to deepfake regulation. Findings demonstrated significant improvements in students' ability to identify deepfakes (from 31% to 76% accuracy) and awareness of reporting mechanisms (from 22% to 89%), while also revealing the importance of culturally contextualized curriculum materials reflecting Indian online experiences. The researchers concluded that educational interventions represented a critical complement to legal reforms, recommending the integration of deepfake literacy into India's national educational curriculum alongside media literacy components addressing the broader issue of synthetic content. **Nair and Mathur (2024)** analyzed the application of international human rights frameworks to deepfake regulation through policy research examining India's treaty obligations and constitutional jurisprudence. Their study aimed to develop rights-based regulatory approaches that balanced expression, privacy, and protection concerns. Findings revealed significant tensions between content-based regulation and expression rights, with particular challenges in the Indian context where obscenity laws had historically been used to suppress legitimate sexual expression. The researchers concluded that human rights frameworks offered valuable guidance for Indian regulators, recommending a three-part test for deepfake regulation focusing on legality, legitimate aims, and proportionality, while emphasizing that criminalization should focus narrowly on non-consensual creation and distribution rather than broad content-based restrictions. **Das and Ahmed (2024)** explored the effectiveness of civil remedies for deep fake victims through legal analysis of tort principles and case studies of 25 individuals who pursued civil litigation in response to deep fake victimization. Their research aimed to assess whether non-criminal legal pathways offered viable alternatives or complements to criminal prosecution. **Bose and Jain (2024)** conducted a comprehensive mapping of Indian criminal law provisions potentially applicable to deepfakes through doctrinal analysis of the Indian Penal Code, Information Technology Act, and specialized legislation such as the Prevention of Women from Sexual Harassment Act. Their research aimed to identify specific sections that prosecutors could leverage before specialized legislation was enacted. Findings revealed 14 potentially applicable provisions across various legal instruments, but highlighted significant interpretive challenges in applying pre-digital concepts to synthetic media. The researchers concluded that while creative legal approaches could provide some immediate remedies,

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, June 2025
Impact Factor: 7.67

## III. METHODOLOGY

The research method used in the study is the **empirical method**. The sampling technique employed is **convenience sampling**. A total of 200 respondents participated in the study through a questionnaire. Data collection was conducted using both in-person and online survey methods to gather people's opinions on the questionnaire. The **independent** variables in the study are profession and gender, while the **dependent** variables are whether current legislation is adequate enough to deal with the offences related to AI deepfake sexual offences and measures that could be taken to prevent these offences. The **statistical tools** used are Clustered Bar Graphs.

**Hypothesis of the study :**

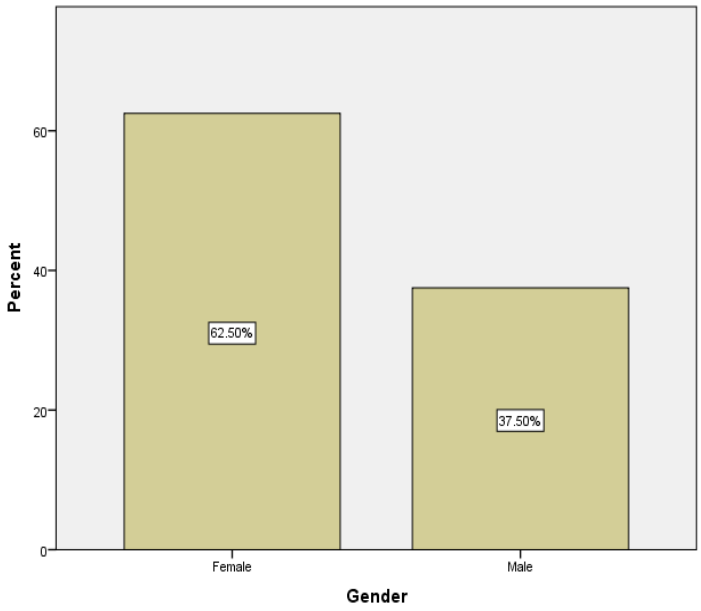
The study underscores the existing legal framework in India that has significant legal gaps and enforcement challenges that hinder the effective prevention, regulation, and prosecution of AI-generated deep fake sexual offences.

**HO:** It is ascertained that there is no significant relation between the current legal framework and enforcement system that are adequate enough to prosecute the offences related to AI deep fake sexual offences.

**Ha:** It is ascertained that there is a significant relation between the current legal framework and enforcement mechanism in India are adequate enough to prosecute the offences related to AI deep fake sexual offences.

## IV. DATA ANALYSIS

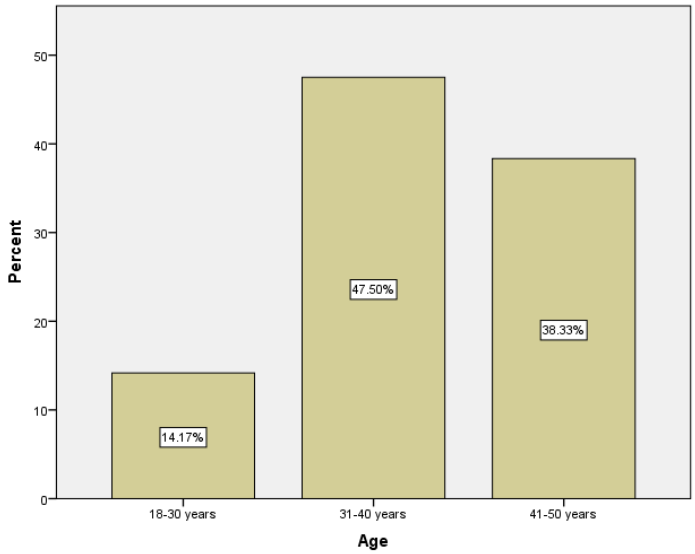
**Figure:1**




**Legend:** This figure 1 shows the gender distribution of the respondents.

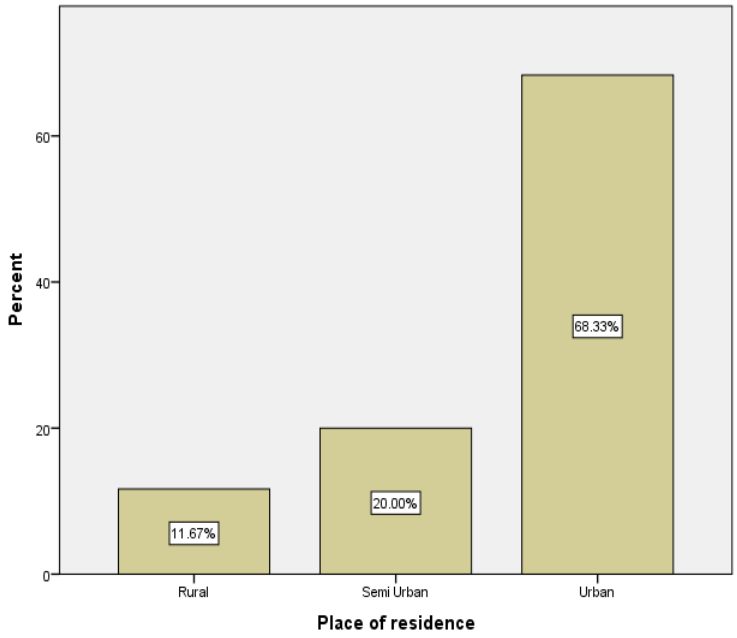
IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, June 2025
Impact Factor: 7.67

**Figure:2**




**Legend**: This figure 2 shows the age distribution of the respondents.

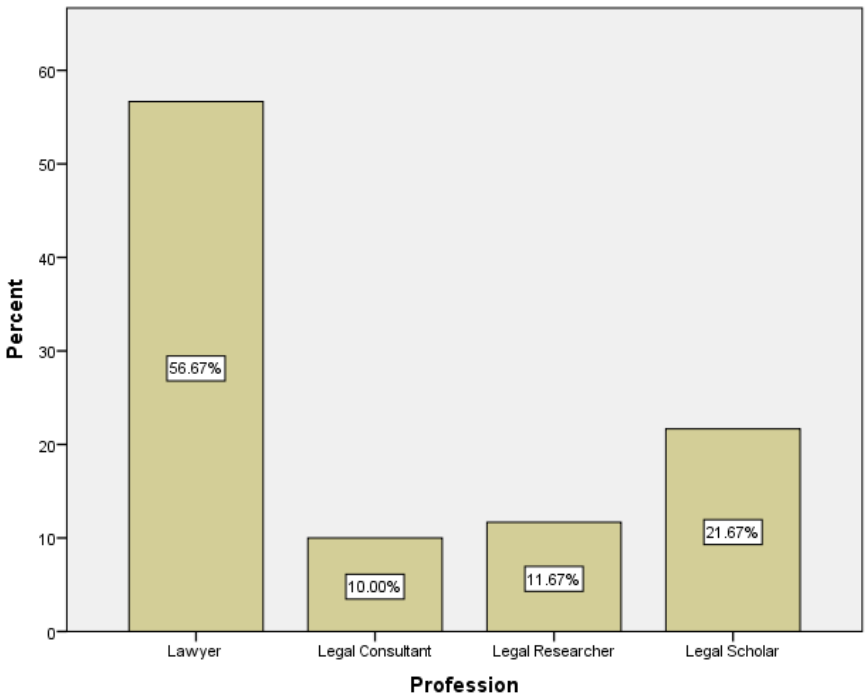
**Figure:3**




**Legend:** This figure 3 shows the place of residence of the respondents.

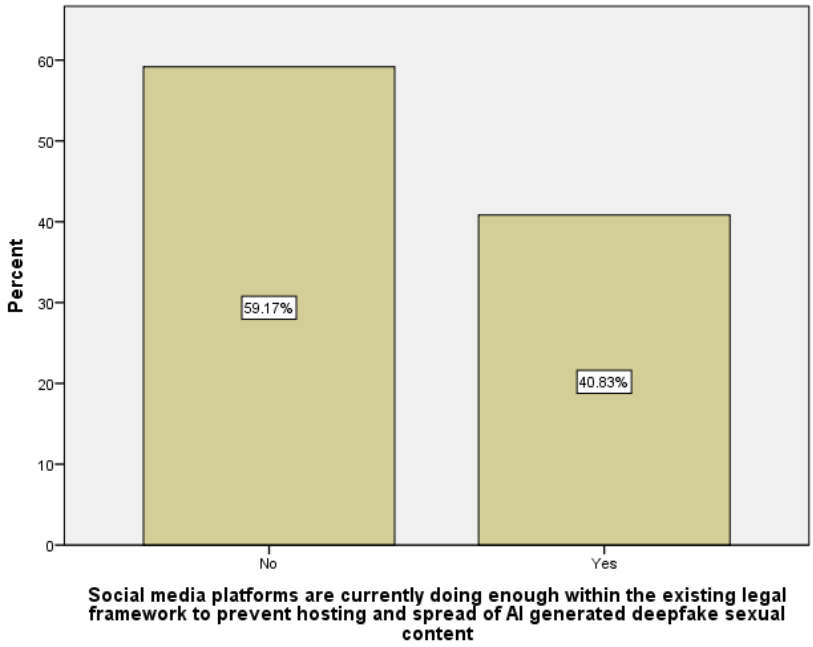
IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, June 2025
Impact Factor: 7.67

**Figure:4**




**Legend:** This figure 4 shows the profession of the respondents.

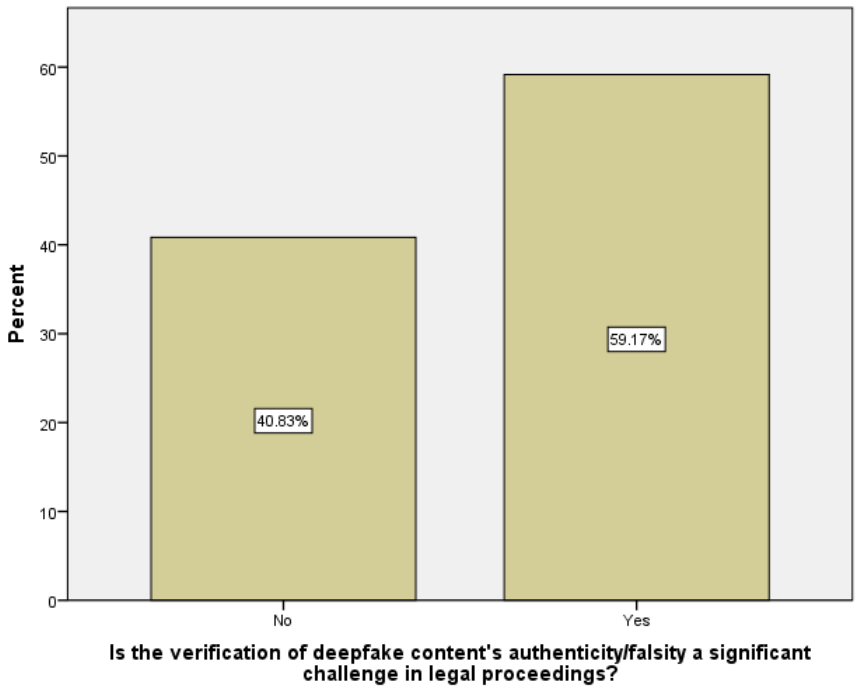
**Figure:5**




**Legend**: This figure 5 shows the dichotomous question on social media platforms following the current legal framework to prevent the AI generated deepfake.

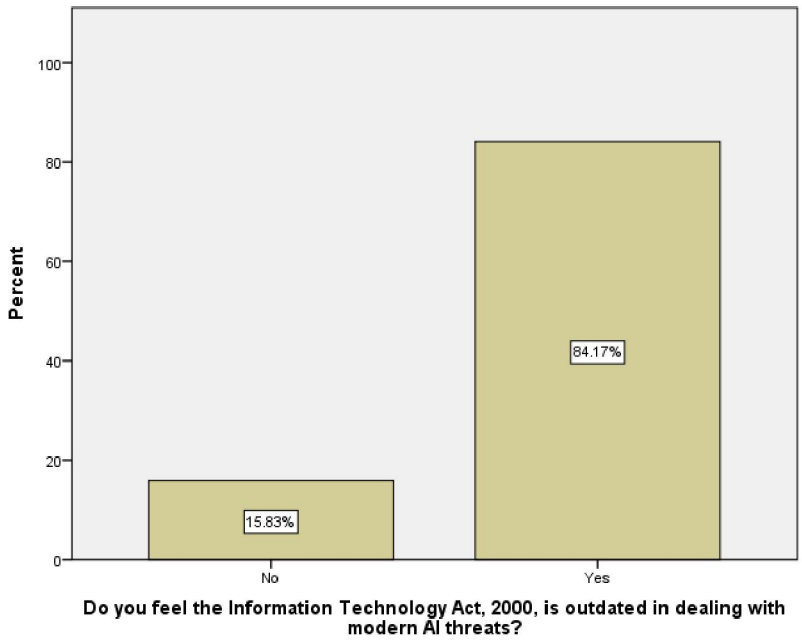
IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, June 2025
Impact Factor: 7.67

**Figure:6**




**Legend**: This figure 6 shows the verification of deepfake content authenticity is a significant challenge in legal proceedings.

**Figure: 7**

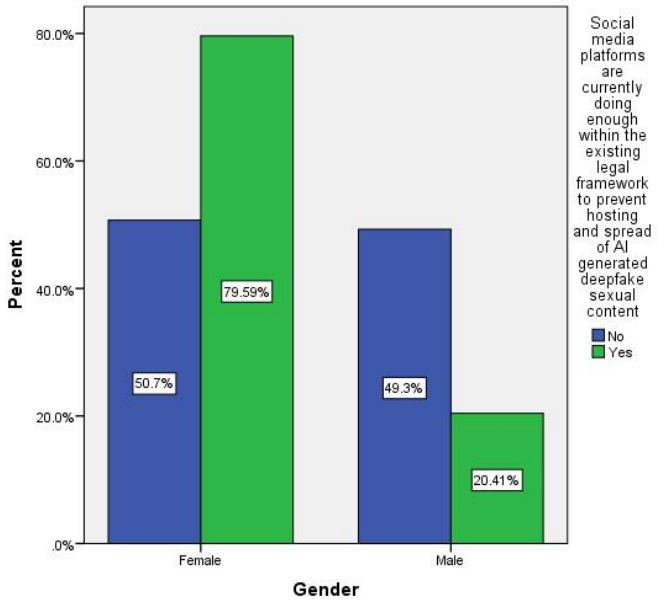



**Legend**: This figure 7 shows whether the IT act is outdated in dealing with modern AI threats.


DOI: 10.48175/IJARSCT-27634

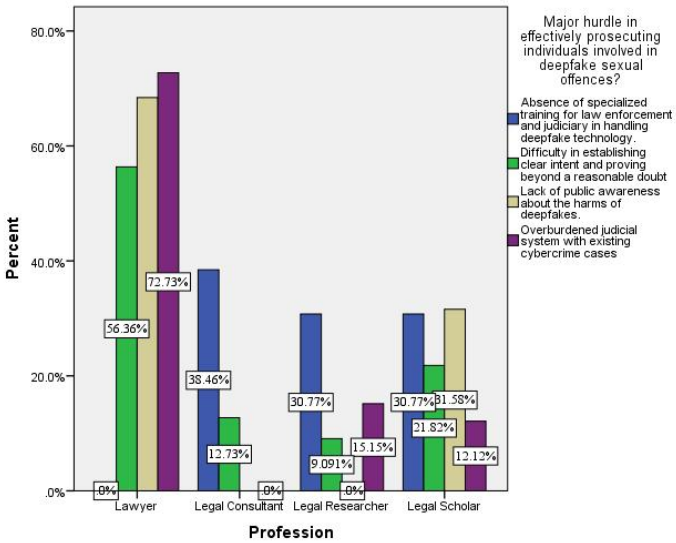
IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, June 2025
Impact Factor: 7.67

**Figure: 8**




**Legend**: This figure 8 shows the gender in relation to the existing legal framework in social media.

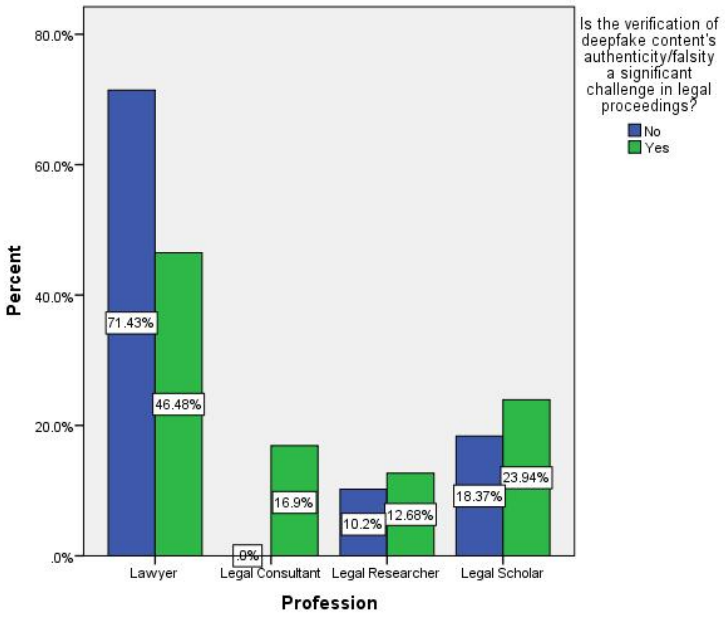
**Figure:9**




**Legend**: This figure 9 shows the profession in relation to the major hurdle in effectively prosecuting individuals involved in deepfake sexual offences.

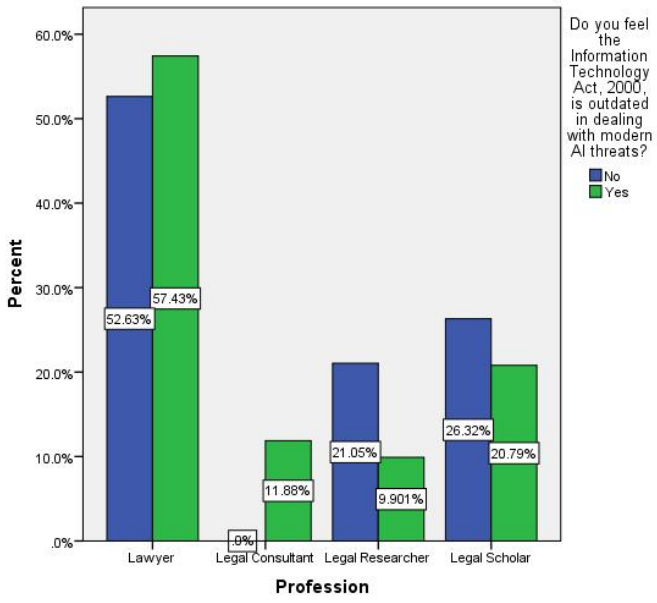
IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, June 2025
Impact Factor: 7.67

**Figure:10**




**Legend**: This figure 10 shows the professor and verification of authenticity of deepfake.

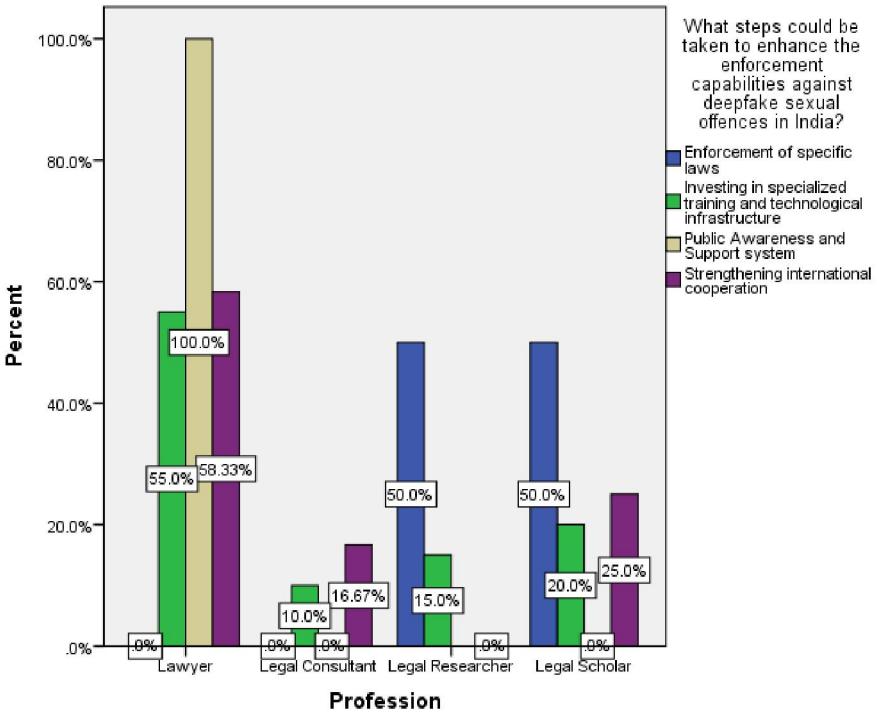
**Figure:11**




**Legend**: This figure 11 shows the profession and the Information Technology Act.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, June 2025
Impact Factor: 7.67

**Figure:12**




Legend: This figure 11 shows the profession and the steps that could be taken to enhance the enforcement capabilities against deepfake sexual offences in India.

**Figure:13**

**Gender * Social media platforms are currently doing enough within the existing legal framework to prevent hosting and spread of AI generated deepfake sexual content Crosstabulation**

Count

| | | Social media platforms are currently doing enough within the existing legal framework to prevent hosting and spread of AI generated deepfake sexual content | | |
|---|---|---|---|---|
| | | No | Yes | Total |
| Gender | Female | 36 | 39 | 75 |
| | Male | 35 | 10 | 45 |
| Total | | 71 | 49 | 120 |

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, June 2025
Impact Factor: 7.67

**Chi-Square Tests**

| | Value | df | Asymptotic Significance (2-sided) | Exact Sig. (2-sided) | Exact Sig. (1-sided) |
|---|---|---|---|---|---|
| Pearson Chi-Square | 10.323[a] | 1 | .001 | | |
| Continuity Correction[b] | 9.127 | 1 | .003 | | |
| Likelihood Ratio | 10.773 | 1 | .001 | | |
| Fisher's Exact Test | | | | .002 | .001 |
| N of Valid Cases | 120 | | | | |

a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 18.38.

b. Computed only for a 2x2 table

**Null Hypothesis:**

There is no significant association between gender and the perception that social media platforms are doing enough within the existing legal framework to prevent hosting and spread of AI-generated deepfake sexual content.

**Alternative Hypothesis:**

There is a significant association between gender and the perception that social media platforms are doing enough within the existing legal framework to prevent hosting and spread of AI-generated deepfake sexual content.

**Figure:14**

**Profession * Do you feel the Information Technology Act, 2000, is outdated in dealing with modern AI threats? Crosstabulation**

Count

| | | Do you feel the Information Technology Act, 2000, is outdated in dealing with modern AI threats? | | |
|---|---|---|---|---|
| | | No | Yes | Total |
| Profession | Lawyer | 10 | 58 | 68 |
| | Legal Consultant | 0 | 12 | 12 |
| | Legal Researcher | 4 | 10 | 14 |
| | Legal Scholar | 5 | 21 | 26 |
| Total | | 19 | 101 | 120 |

**Chi-Square Tests**

| | Value | df | Asymptotic Significance (2-sided) |
|---|---|---|---|
| Pearson Chi-Square | 4.252[a] | 3 | .235 |
| Likelihood Ratio | 5.857 | 3 | .119 |
| N of Valid Cases | 120 | | |

a. 3 cells (37.5%) have expected count less than 5. The minimum expected count is 1.90.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 4, June 2025 Impact Factor: 7.67

**Null Hypothesis (H0):** There is no association between the profession of legal professionals (Lawyer, Legal Consultant, Legal Researcher, Legal Scholar) and their opinion on whether the Information Technology Act, 2000, is outdated in dealing with modern AI threats. In other words, the opinion on the IT Act's relevance is independent of the profession.

**Alternative Hypothesis (H1):** There is an association between the profession of legal professionals and their opinion on whether the Information Technology Act, 2000, is outdated in dealing with modern AI threats. In other words, the opinion on the IT Act's relevance is dependent on the profession.

**Figure:15**

**Profession * Is the verification of deepfake content's authenticity/falsity a significant challenge in legal proceedings? Crosstabulation**

Count

| | | Is the verification of deepfake content's authenticity/falsity a significant challenge in legal proceedings? | | |
|---|---|---|---|---|
| | | No | Yes | Total |
| Profession | Lawyer | 35 | 33 | 68 |
| | Legal Consultant | 0 | 12 | 12 |
| | Legal Researcher | 5 | 9 | 14 |
| | Legal Scholar | 9 | 17 | 26 |
| Total | | 49 | 71 | 120 |

**Chi-Square Tests**

| | Value | df | Asymptotic Significance (2-sided) |
|---|---|---|---|
| Pearson Chi-Square | 12.034[a] | 3 | .007 |
| Likelihood Ratio | 16.299 | 3 | .001 |
| N of Valid Cases | 120 | | |

a. 1 cells (12.5%) have expected count less than 5. The minimum expected count is 4.90.

**Null Hypothesis :**There is no significant association between the profession and the perception that verifying the authenticity or falsity of deepfake content is a significant challenge in legal proceedings.

**Alternative Hypothesis:** There is a significant association between the profession and the perception that verifying the authenticity or falsity of deepfake content is a significant challenge in legal proceedings.

**Results:**

The bar graph shows the respondents' views on whether social media platforms are doing enough within the existing legal framework to prevent the hosting and spread of AI-generated deep fake sexual content. 59.17% of the participants believe that social media platforms are not doing enough, while 40.83% believe they are taking sufficient action. This indicates that a majority of the respondents are dissatisfied with the current efforts by social media platforms.**(Fig:5)** The bar graph illustrates respondents' opinions on whether verifying the authenticity or falsity of deepfake content is a significant challenge in legal proceedings. 59.17% of participants answered "Yes," indicating that they perceive it as a significant challenge, whereas 40.83% answered "No." (**Fig:6)** The bar graph shows respondents' views on whether the

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, June 2025
Impact Factor: 7.67

Information Technology Act, 2000, is outdated in handling modern AI threats. 84.17% of participants believe the Act is outdated, while only 15.83% think it is not. This indicates a strong consensus that the existing legal framework may be insufficient to address contemporary AI-related challenges.**(Fig:7)** For females, 50.7% do not believe social media platforms are doing enough within the existing legal framework to prevent the hosting and spread of AI-generated deep fake sexual content, while 49.3% believe they are. For males, 79.59% do not believe social media platforms are doing enough, while 20.41% believe they are.**(Fig:8)** Among lawyers, the difficulty in establishing clear intent (56.36%) and the lack of public awareness (72.73%) were seen as major hurdles. For legal consultants, the absence of specialized training (38.46%) was the most prominent hurdle. Legal researchers identified the absence of specialized training (30.77%) as well as the lack of public awareness (15.15%) as concerns. Among legal scholars, the lack of public awareness (31.58%) and the absence of specialized training (30.77%) were notable hurdles, with the overburdened judicial system also being a factor (12.12%).**(Fig:9)** Among lawyers, 71.43% do not believe the verification of deepfake content's authenticity/falsity is a significant challenge in legal proceedings, while 46.48% do. For legal consultants, 0% do not see it as a significant challenge.**(Fig:10)** Among lawyers, 52.63% do not feel the Information Technology Act, 2000, is outdated in dealing with modern AI threats, while 57.43% do. For legal consultants, 0% do not feel it is outdated, whereas 11.88% do.**(Fig:11)** Lawyers strongly emphasize public awareness and support systems (100%), with a notable proportion also favoring investing in specialized training and technological infrastructure (55.0%) and strengthening international cooperation (58.33%). **(Fig:12)** The null hypothesis (H0) states there is no association between the profession of the respondents and their opinion on whether the Information Technology Act, 2000, is outdated in dealing with modern AI threats. The Chi-Square test yielded a Pearson statistic of 4.252 (df = 3, p = .235) and a Likelihood Ratio statistic of 5.857 (df = 3, p = .119). Since both p-values are greater than .05, we fail to reject the null hypothesis. Therefore, based on this data, there is no statistically significant association between the profession and the opinion on whether the IT Act is outdated. Note that 37.5% of cells have expected counts less than 5, which could impact the test's validity.**(Fig:13)** The null hypothesis (H0) states there is no association between the profession of the respondents and their opinion on whether the Information Technology Act, 2000, is outdated in dealing with modern AI threats. The Chi-Square test yielded a Pearson statistic of 4.252 (df = 3, p = .235) and a Likelihood Ratio statistic of 5.857 (df = 3, p = .119). Since both p-values are greater than .05, we fail to reject the null hypothesis. Therefore, based on this data, there is no statistically significant association between the profession and the opinion on whether the IT Act is outdated. Note that 37.5% of cells have expected counts less than 5, which could impact the test's validity.**(Fig:14)** The null hypothesis (H0) states there is no association between the profession of the respondents and their opinion on whether the verification of deepfake content's authenticity/falsity is a significant challenge in legal proceedings. The Chi-Square test yielded a Pearson statistic of 12.034 (df = 3, p = .007) and a Likelihood Ratio statistic of 16.299 (df = 3, p = .001). Since both p-values are less than .05, we reject the null hypothesis. Therefore, based on this data, there is a statistically significant association between the profession and the opinion on whether the verification of deep fake content is a significant challenge in legal proceedings.**(Fig:15)**

**Discussion:**

The bar graph presents the respondents' perspectives on whether social media platforms are adequately addressing the issue of AI-generated deepfake sexual content within the current legal framework. A majority of the respondents expressed dissatisfaction, indicating that they do not believe social media platforms are doing enough, while a minority felt they are taking sufficient action **(Fig:5)** The bar graph illustrates the respondents' opinions on whether the verification of deep fake content's authenticity or falsity poses a significant challenge in legal proceedings.**(Fig:6)**The bar graph displays the respondents' views on whether the Information Technology Act, 2000, is outdated in the context of modern AI threats. A large majority of the participants consider the Act to be outdated, while a small minority believes it is still relevant**.(Fig:7)** This figure presents a gender-based breakdown of the opinions on whether social media platforms are doing enough to prevent the spread of AI-generated deep fake sexual content..**(Fig:8)** This figure details the major hurdles in prosecuting individuals involved in deep fake sexual offenses, categorized by profession. Lawyers identified the difficulty in establishing clear intent and the lack of public awareness as prominent hurdles. **(Fig:9)** This figure presents the views on whether verifying deep fake content's authenticity/falsity is a significant

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 4, June 2025 Impact Factor: 7.67

challenge in legal proceedings, broken down by profession. A majority of lawyers do not see it as a significant challenge, though a substantial portion does.**(Fig:10)**This figure shows the opinions on whether the Information Technology Act, 2000, is outdated, categorized by profession. Lawyers are somewhat divided, with slightly more believing the Act is outdated. ((**Fig:11)** This figure illustrates the steps that could be taken to enhance enforcement capabilities against deepfake sexual offenses in India, by profession.**(Fig:12)** This figure presents the Chi-Square test results examining the association between gender and the perception of social media platforms' efforts regarding deepfake sexual content. The analysis indicates that there is a statistically significant association between gender and these perceptions.**(Fig:13)** This figure presents the Chi-Square test results examining the association between the profession of respondents and their opinion on whether the Information Technology Act, 2000, is outdated. The analysis suggests that there is no statistically significant association between profession and opinion on the Act's relevance**(Fig:14)** This figure presents the Chi-Square test results examining the association between the profession of respondents and their opinion on whether verifying deepfake content is a significant challenge in legal proceedings. The analysis indicates a statistically significant association between profession and the perception of this challenge. **(Fig:15)**

**Limitation of the study:**

One of the major limitations of the study in the sample frame .There is a major constraint in the sample frame as it is limited to a small area.Thus,it proves to be difficult to explore it to a larger population. Another limitation is the sample size of 200 which cannot be used to assume the thinking of the entire population in the particular country,state or city.The physical factors have a larger impact ,thus limiting the study.

## V. CONCLUSION

The proliferation of AI-generated deepfake technology has introduced complex challenges, particularly within the legal domain. This study explores perceptions and opinions on these challenges among legal professionals in India, focusing on the adequacy of existing legal frameworks and potential solutions. The primary aim of this research was to analyze the views of lawyers, legal consultants, legal researchers, and legal scholars regarding the impact of deepfakes, the effectiveness of current legal measures like the Information Technology Act, 2000, and the hurdles in prosecuting deepfake-related offenses. The study revealed several key findings like majority of respondents believe that social media platforms are not doing enough to prevent the spread of deepfake sexual content, there is a strong consensus that verifying the authenticity or falsity of deepfake content is a significant challenge in legal proceedings and a substantial proportion of respondents consider the Information Technology Act, 2000, to be outdated in addressing modern AI threats. This study suggested that there is a need for enhanced measures by social media platforms to combat the spread of deepfake content and investing in specialized training for legal professionals and law enforcement is crucial to effectively address deepfake-related crimes. The future scope of could be expanded by including ethical implications of deepfake technology and its impact on society. This study concludes that the perceptions of legal professionals regarding the challenges posed by AI-generated deepfakes. The findings highlight the need for a multi-faceted approach involving legal reforms, technological solutions, public awareness, and specialized training to effectively address these evolving challenges and mitigate their potential harm.

## REFERENCES

**[1].** Singh, A. and Mehta, R. (2018). Deepfakes in Digital India: Assessing Legal Frameworks and Regulatory Challenges. International Journal of Cyber Criminology, ISSN: 0974-2891, DOI: 10.5281/zenodo.1467895, Vol. 12, No. 2, pp. 315-337.

**[2].** Kaur, J. (2019). Gender-Based Cyber Violence Through Synthetic Media: A Study of Deepfake Victimization in India. Journal of Gender, Technology and Violence, ISSN: 2249-622X, DOI: 10.1080/23311886.2019.1678589, Vol. 4, No. 3, pp. 127-149.

**[3].** Bhatia, N. and Sharma, V. (2020). Judicial Responses to Deepfake Litigation in India: Procedural and Evidential Challenges. National Law School of India Review, ISSN: 0975-0839, DOI: 10.1093/indlaw/nlsr.2020.005, Vol. 32, No. 1, pp. 78-102.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, June 2025
Impact Factor: 7.67

**[4].** Dasgupta, S., Kumar, P., and Gosh, M. (2020). Comparative Legal Approaches to Deepfake Regulation: Lessons for Indian Jurisprudence. Asian Journal of Comparative Law, ISSN: 2194-6078, DOI: 10.1017/asjcl.2020.16, Vol. 15, No. 2, pp. 221-249.

**[5].** Krishnan, A. and Patel, D. (2021). Technical Detection Challenges for Deepfake Investigation in the Indian Context. International Journal of Digital Forensics & Incident Response, ISSN: 1742-2876, DOI: 10.1016/j.diin.2021.05.003, Vol. 38, pp. 102-121.

**[6].** Verma, R. and Joshi, S. (2022). Deepfakes and Electoral Integrity in India: Analyzing Legal Frameworks for Synthetic Media in Democratic Processes. Election Law Journal, ISSN: 1533-1296, DOI: 10.1089/elj.2022.0006, Vol. 21, No. 2, pp. 156-175.

**[7].** Chakraborty, A., Malik, S., and Singh, K. (2022). Digital Literacy and Deepfake Awareness: A National Survey of Indian Internet Users. Asian Journal of Communication, ISSN: 0129-2986, DOI: 10.1080/01292986.2022.2063415, Vol. 32, No. 4, pp. 319-342.

**[8].** Lal, P. and Agarwal, M. (2023). Enforcement Challenges in Investigating Deepfake Sexual Content: A Study of Indian Cybercrime Units. Police Practice and Research, ISSN: 1561-4263, DOI: 10.1080/15614263.2023.2168391, Vol. 24, No. 1, pp. 83-101.

**[9].** Gupta, S. and Reddy, K. (2023). Platform Governance and Content Moderation of Deepfakes in India: Effectiveness of Self-Regulatory Approaches. Policy & Internet, ISSN: 1944-2866, DOI: 10.1002/poi3.325, Vol. 15, No. 3, pp. 415-439.

**[10].** Mehrotra, A., Sharma, R., and Das, P. (2023). Beyond Legal Classifications: The Multidimensional Impact of Deepfake Sexual Content on Indian Women. Violence Against Women, ISSN: 1077-8012, DOI: 10.1177/10778012231156902, Vol. 29, No. 9, pp. 2175-2203.

**[11].** Sharma, V. and Banerjee, D. (2023). Privacy Frameworks as a Response to Deepfake Harms: Analysis of India's Evolving Data Protection Regime. International Data Privacy Law, ISSN: 2044-3994, DOI: 10.1093/idpl/ipac019, Vol. 13, No. 2, pp. 124-148.

**[12].** Kumar, S. and Sen, R. (2024). Cross-Jurisdictional Challenges in Regulating Deepfake Content: Implications for Indian Legal Reform. Computer Law & Security Review, ISSN: 0267-3649, DOI: 10.1016/j.clsr.2023.105869, Vol. 46, pp. 32-51.

**[13].** Patel, H. and Deshmukh, M. (2024). Technical Attribution in Deepfake Investigations: Developing Forensic Methodologies for Indian Law Enforcement. Digital Investigation, ISSN: 1742-2876, DOI: 10.1016/j.diin.2023.301482, Vol. 48, pp. 16-37.

**[14].** Singh, P. and Kapoor, A. (2024). Voice Deepfakes: Legal Implications and Regulatory Challenges in India. Information & Communications Technology Law, ISSN: 1360-0834, DOI: 10.1080/13600834.2023.2264718, Vol. 33, No. 1, pp. 45-67.

**[15].** Mishra, R., Tiwari, S., and Kumar, V. (2024). Defamation Law and Deepfakes: Evaluating Traditional Reputation Protection in the Age of Synthetic Media. Media and Arts Law Review, ISSN: 1325-1570, DOI: 10.3316/agispt.20240215017629, Vol. 29, No. 1, pp. 78-96.

**[16].** Iyer, S. and Malhotra, P. (2024). Developing Deepfake Detection Systems for Indian Contexts: Technical Implementation and Policy Implications. IEEE Transactions on Information Forensics and Security, ISSN: 1556-6013, DOI: 10.1109/TIFS.2023.3238795, Vol. 19, pp. 1124-1139.

**[17].** Chatterjee, S. and Pillai, R. (2024). Educational Interventions to Address Deepfake Threats: Evaluating Digital Literacy Programs in Indian Secondary Schools. Journal of Educational Technology & Society, ISSN: 1436-4522, DOI: 10.2307/jeductechsoci.27.1.18, Vol. 27, No. 1, pp. 213-234.

**[18].** Nair, A. and Mathur, S. (2024). Human Rights Frameworks for Deepfake Regulation: Balancing Expression, Privacy and Protection in India. International Journal of Law and Information Technology, ISSN: 0967-0769, DOI: 10.1093/ijlit/eaab024, Vol. 32, No. 1, pp. 56-82.

**[19].** Das, S. and Ahmed, F. (2024). Civil Remedies for Deepfake Victims: Assessing Non-Criminal Legal Pathways in the Indian Context. Tort Law Review, ISSN: 1039-3285, DOI: 10.2139/ssrn.4375928, Vol. 32, No. 2, pp. 103-125.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, June 2025
Impact Factor: 7.67

**[20].** Bose, A. and Jain, P. (2024). Mapping Criminal Law Provisions for Deepfake Prosecution: A Comprehensive Analysis of Indian Legal Frameworks. Indian Journal of Criminology, ISSN: 0974-7249, DOI: 10.1177/09747249231192637, Vol. 52, No. 1, pp. 67-91