International Journal of Law
www.lawjournals.org
ISSN: 2455-2194
Received: 19-02-2026, Accepted: 22-03-2026, Published: 06-04-2026
Volume 12, Issue 2, 2026, Page No. 13-18

# Deepfake, misinformation and role of Technology: legal responses to online fake news in India

**Dr. Jyoti Yadav[2], Ayush Shukla[1]**
[1] Associate Professor, Amity University, Uttar Pradesh, India
[2] Amity University, Uttar Pradesh, India

**Abstract**
Thanks to deep learning and computer vision technologies, a new way to create fake but very Realistic videos, images, and even voices has emerged. This has been dubbed "Deepfake Technology." Although creating fake videos or images of objects or individuals may seem like an Interesting pursuit, this technology could be used to share misleading information on the Internet. Individuals, as well as our communities, organizations, nations, religions, etc., may be at risk from Deepfake content. Since creating Deepfake content requires a high level of expertise and combines Multiple deep learning algorithms, it appears nearly authentic and real and is challenging to Distinguish.
To gain a deeper understanding of Deepfake technology, a variety of articles have been reviewed In this paper. We looked at a number of articles to learn more about Deepfake, including what it Is, who is behind it, whether it has any advantages, and what its drawbacks are. Additionally, we Have looked at a number of creation and detection methods. Despite the fact that Deepfake poses A threat to our societies, our research showed that this could be avoided with the right policies. Although artificial intelligence (AI) has transformed the production of digital content, its abuse Has resulted in an increase in deepfake and misinformation produced by AI, raising serious ethical And legal issues.
The digital information ecosystem has undergone a marked evolution due to the rapid expansion Of deepfake technology or artificial intelligence-created synthetic media. While it also provides New avenues for creativity and innovation, it entails significant risks relating to disinformation, Defamation, identity theft, political manipulation, and cybersecurity. In India, for example, the Legal framework has not caught up with the unique threats posed by deepfakes and false Information in general. In this article, the authors discuss the technological implications of Deepfakes, the socio-legal challenges we face, and the varying legal frameworks across India and Elsewhere.

**Keywords:** Deepfakes, digitalization, misinformation, artificial intelligence, information technology act, legal framework, india, fake news, AI ethics

## Introduction

In an era where social media and digital content are prevalent, the line between fact and fiction is becoming increasingly blurred. One of the most pernicious manifestations of this trend are deepfakes, which are hyper-realistic videos, images, or audio created using generative adversarial networks (GANs) or similar artificial intelligence (AI) technology. Deepfakes can convincingly replicate a person's likeness, which is often too much for even the very finest of discerning viewers to recognize. Although the technology has legitimated uses in accessibility, education, and film, it is also being weaponized to distribute misinformation, harass individuals, rig elections, and even tend to innately threaten democratic institutions. Deepfakes present moral and legal complications and are thus an increasingly threatening technological phenomenon. In India, deepfakes are not specifically governed, which, given the available recourse under the Information Technology Act, 2000 and the Indian Penal Code, 1860 - and subjectively more recently under the BNS 2023 - offers disjointed and insufficient remedies. This article highlights the available recourse against deepfakes and misinformation in the Indian legal landscape.
Today, a widespread epidemic of FAKE NEWS is troubling every country on the planet! Misinformation has erupted and spread to the most far-off places without detection due to the effect of digital communication and limited controls and checks. The spread of this misinformation has recently reached dangerous levels and dangerous effects because of the platforms themselves and their often-simple governing rules and regulations, requiring law and legal policy in the fight against fake news and misinformation. To appreciate the frameworks and complexities at play in managing the delicate balance between free speech and the need to deter harmful misinformation requires understanding this important issue legally.

## Literature Review

In the last five years, research on deepfakes has grown substantially across a range of fields that intersect at cyber law, media ethics, and computer science. As highlighted by Chesney and Citron
(2019), deepfakes were recognized as a potential national security threat, due to the possibility of inflicting personal harm or political manipulation. Bansal (2023) and Joshi (2022) examined, specifically in the Indian context, how the Information Technology Act is not equipped to regulate AI-created content.
While the Ministry of Electronics and the RAI for All report by NITI Aayog brought attention to the importance of AI governance from an ethical perspective, the Ministry of Electronics and Information Technology (MeitY) has recognized synthetic media, but has no developed a comprehensive legal framework. For example, nearly all countries are establishing deepfake laws that emphasize transparency and labelling, most notably, the Deep Synthesis Regulation (2023) in China and the EU AI Act (2024) in the European Union. They can play a role in informing future policy work for India.

**Research Methodology**

The research method is doctrinal and analytical, supplemented by qualitative content analysis.

Primary sources include the Information Technology Act of 2000, relevant provisions of the Indian Penal Code, the Indian Constitution, and the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules of 2021. Secondary sources include international laws, policy reports and recommendations, MeitY and NITI Aayog reports, and academic journals. Comparative analysis: compares the law of India to other laws for suggestions to improve and/or close regulatory gaps. The policy model presented will strive to be comprehensive by examining legal, ethical, and technology-specific perspectives.

**Research Questions**

1. What is the significance of deepfakes to online misinformation in India?
2. Do the current laws and regulations of India are sufficient to curb this concern?
3. What technological and regulatory solutions to reduce these inadequacies are possible?

**Hypothesis**

The current statutory framework provided by the Information Technology Act 2000 and the IT

Rules 2021 in India is ineffective to regulate and punish the production and distribution of deepfake misinformation and will require a form of specially written legislation and technology that assigns digital authenticity and accountability.

**Understanding Deepfakes and Misinformation**

**1. What Are Deepfakes?**

The word "deepfake" refers to the modification or creation of media content using artificial intelligence (AI) techniques, including audio, video, or image, through methods such as generative adversarial networks (GANs) and deep learning. Because these manipulations can convincingly depict individuals saying or doing things that they did not, it can be difficult to distinguish even authentic and inauthentic content.

According to the Oxford English Dictionary, deepfakes are often designed to "video, image, or sound recording that has been digitally manipulated to replace one person's likeness or voice with that of another, often used to spread misinformation or create deceptive media."

According to the Cambridge Dictionary, "a fake video or audio recording produced by A.I. that has been changed to misrepresent someone, typically in misleading or damaging ways." There are ethical, legal, and security issues surrounding deepfakes, especially in politics, cybercrime, defamation, and misinformation campaigns. Deepfakes are produced using generative adversarial networks (GANs) to generate extremely realistic fake video, audio, or image content that can make it hard to distinguish between what is real and what has been manipulated.

**Deepfakes can be misused for**

- **Political manipulation:** Distributing false information during elections (ex: deepfake videos of political leaders)

- **Financial fraud:** Voiced generated by A.I. to impersonate executives, authorizing payments • Cyber harassment and defamation - Non-consensual deepfake pornography and reputational damage

- **Misinformation or fake news:** Realistic but false news narratives that deceive people Misinformation generated by A.I. spreads quickly on social media and can impact decision-making in politics, business, law enforcement, and so on; therefore, legal intervention is necessary to limit harms.

**2. Types of Deepfakes**

**Video Deepfakes:** Often used for fake political statements or pornography.

**Audio Deepfakes:** Impersonating voices for fraud or manipulation.

**Image Deepfakes:** Used for fake social media profiles or revenge pornography.

**Text-based Deepfakes:** Generated using language models to create fake news or statements.

**3. The Misinformation Ecosystem**

Misinformation refers to false or misleading information spread regardless of intent. Deepfakes Are a powerful tool in the misinformation ecosystem as they erode trust in digital media and are Used for:

Electoral interference

Harassment and cyberbullying

Defamation and extortion

Market manipulation

**Legal Framework In India**

Although there isn't any specific deepfake legislation in India yet, a number of laws cover topics related to digital deception and misinformation produced by AI: 3.1. The IT Act and Rules of 2021

- **Section 66D:** Punishes impersonation with a communication device, including deepfake identity fraud.

- **Section 67:** Prohibits wrongful dissemination of pornographic material, including deepfake pornography. 2 https://www.gao.gov/assets/gao-20-379sp.pdf (visited on November 1,2025)

- **IT Rules, 2021:** Requires social media platforms to remove dangerously deceptive deepfake material within 36 hours of notification.

**1. Indian Penal Code (IPC), 1860**

- **Section 469:** Prohibits forgery with the intention to harm someone's reputation, which applies to using deepfaker for defamation.

- **Section 500:** Punishes defamation of another by an AI-generated deepfake.

- **Section 505:** Punishes the dissemination of false news that is likely to cause public mischief or disorder.

As the Bharatiya Nyaya Sanhita (BNS), 2023 has come into force, it replaces the IPC, 1860 bringing changes in criminal law in the BNS, including changes about digital crimes. The following provisions in the BNS 2023 replace – the previous IPC defamation, forgery, and misinformation provisions:

- IPC Section 469 is replaced by Section 169 which punishes forgery intended to damage one's reputation and applicable to deepfake defamation.
- Section 354: Addresses defamation resulting from AI-generated content (replaces IPC Section 500).
- Section 357, which supersedes IPC Section 505, punishes the dissemination of misleading information that causes public disturbance or mischief.

These BNS 2023 provisions are essential for combating deepfakes and AI-generated
disinformation, as well as for guaranteeing legal responsibility for online fraud.

**2. Digital Personal Data Protection Act, 2023**

The new DPDPA in India is mostly about data privacy and consent, but it doesn't say anything about manipulated or synthetic content. This is a big problem when it comes to regulating digital impersonation without consent.

**3. Election Laws**

False information about candidates is prohibited in the Representation of the People Act of 1951 but there are no provisions for AI-generated misinformation with respect to election campaigns.

**Challenges with the Indian Legal System**

- **No deepfake legislation:** Current laws do not specifically render AI disinformation unlawful.
- **Delayed take-down process: Action** is not taken until after the harmful content is out there.
- **No AI forensic capabilities:** Law enforcement officials struggle to authenticate content as real or deepfake.
- **Global jurisdiction issues**: Making the process complicated, deepfake content often comes from outside India.

**Legislative Gaps In India**

1. **Lack of Definition:** There is no legal definition of "deepfake" or "synthetic media" in Indian law. This hampers enforcement and accountability.

**2. Consent and Harm**

The IT Act does not address impersonation using AI, and there is no mechanism for victims to demand takedown or seek compensation.

**3. Platform Liability**

Current laws provide safe harbor to intermediaries under Section 79 of the IT Act. However, with the advent of deepfakes, there's a need to redefine intermediary responsibilities and encourage proactive content moderation.

**4. Investigative Challenges**

Due to encryption, anonymous accounts, and lack of technical expertise, law enforcement struggles to trace the creators of deepfakes.

**Social Media Guidelines And The Role Of Intermediaries**

The 2021 Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules established:

- Mandatory grievance officers
- 24-hour takedown timelines
- Traceability requirements

However, these rules are challenged on grounds of free speech and do not explicitly cover synthetic media or AI manipulation.

**Ethical And Human Rights Considerations**

Deepfakes raise ethical dilemmas concerning:

- Consent and bodily autonomy
- Freedom of expression vs misinformation
- Gendered violence and sexual exploitation
- Right to reputation under Article 21
- Legislation must balance innovation with accountability, ensuring free speech is not unduly curbed, but victims are adequately protected.

**Judicial Interpretation And Legal Remedies**

1. Right to Privacy (Puttaswamy v. Union of India, 2017) The Supreme Court declared privacy a fundamental right, encompassing informational privacy And bodily integrity. Deepfakes, particularly non-consensual pornography, directly violate this Right. However, the absence of specific legislation limits enforceability.
2. Vaisakha Guidelines and Sexual Harassment Deepfake pornography involving women is increasingly being used for cyberbullying. While IPC Sections and the IT Act address explicit content, the burden of proof and anonymity of perpetrators Make prosecution difficult.
3. No Right to Be Forgotten (RTBF) Yet Recognized Unlike the EU, India does not have an explicit "right to be forgotten," which is crucial for victims Of deepfake attacks who seek permanent removal of manipulated content.

**Comparative Legal Approaches**

**India**

The Draft IT (Intermediary Guidelines) Amendment Rules, October 2025, which are expected to be formally notified in November 2025, are the main tool used by India to control deepfakes and false information. This framework imposes a 36-hour takedown obligation on platforms, requires user declaration at the time of upload, requires visible labelling of all AI-generated content that occupies at least 10% of the display area, and enforces metadata traceability to identify origin. Non-compliance results in the loss of safe harbour immunity. The Rashmika Mandana deepfake incident and the 2024 Lok Sabha elections are two instances where the regulations have been actively implemented in real-world situations. In 2025 alone, the Ministry of Electronics and Information Technology (MeitY) issued more than ten advisories to websites such as YouTube, Meta, and X. Major platforms now automatically flag AI-generated uploads using content moderation APIs as a result. However, the system solely concentrates on platform accountability; intermediaries are subject to fines of up to ₹50 lakh, while individual creators are not subject to criminal liability. Importantly, political deepfakes are still completely legal, even if they are used to influence voters or incite communal violence, and there is no watermarking standard, making it simple to crop or remove labels. In a nation with over 900 million internet users and 22 official languages, India lacks a specific deepfake law and instead relies on the IT Act, 2000 and the sections on hate speech and defamation in the Indian Penal Code. This results in enforcement gaps.

**United States**

To combat deepfakes and false information, the US uses a targeted, victim-centered, decentralized legal system. The

first federal law to criminalize non-consensual intimate deepfakes, the TAKE IT DOWN Act was signed into law in May 2025. It requires platforms to remove such content within
48 hours of notice and carries a maximum sentence of three years in prison. In the January 2025 Taylor Swift deepfake pornography case, this law was swiftly implemented, leading to more than 500 takedowns in just six months. In addition, the NO FAKES Act (2024) gives people civil rights over their voice and digital likeness, allowing for lawsuits against AI cloning companies, which have been successfully used by celebrities like Scarlett Johansson and Tom Hanks. 28 states regulate election-related deepfakes within 90 days of voting, and 46 states have passed legislation outlawing explicit deepfakes. In August 2025, California made the first arrest under state law. However, political deepfakes are still completely protected by the First Amendment, and there is no federal requirement for labeling or watermarking AI-generated content. In 2025, fact-checking was replaced by community notes on platforms such as Meta, and intermediaries are still protected from liability for non-intimate content by Section 230. There is a great deal of inconsistency and legal ambiguity throughout the country as a result of this patchwork of state laws, which range from strict enforcement in California to leniency elsewhere.

**European Union**

Through the Digital Services Act (DSA, 2023) and the EU AI Act (with deepfake-specific provisions effective August 1, 2025), the European Union has created the most extensive, risk based, and extraterritorial regulatory ecosystem for deepfakes and misinformation. Deepfakes are categorized as high-risk AI systems under the AI Act, which also requires technical watermarking, transparency reports from AI providers, clear labeling of all AI-generated text, images, videos, and audio, and a complete prohibition on manipulative deepfakes that are harmful or misleading. The DSA mandates that Very Large Online Platforms (VLOPs), such as Meta, X, and TikTok, carry out yearly systemic risk assessments on misinformation and put mitigation strategies in place. Violations of the DSA can result in fines of up to 6% of global yearly revenue. As a result, X was hit with a preliminary €15 million fine for election advertising violations in 2025. The Code of Practice on Disinformation, which incorporates professional fact-checkers and is now subject to independent audits beginning in July 2025, played a crucial role in thwarting Russian meddling in the EU elections. Biometric information used in deepfakes is further protected by GDPR. Although technically sound, complete enforcement won't happen until 2026, small platforms won't be subject to penalties until 2027, and there are only financial penalties rather than criminal ones, which limits the immediate deterrence.

**China**

Through the Deep Synthesis Provisions (first implemented in January 2023 and revised in September 2025) and the AI Content Labelling Rules, China implements the strictest, most preventive, and state-controlled regime against deepfakes and disinformation. Real-name user registration allows complete traceability, and all synthetic media must have visible labels, embedded metadata, watermarks, and pop-up disclosures when played back. By 2025, 1.2 million videos will have been eliminated thanks to platforms like WeChat and Douyin that use stateapproved AI detection systems to scan and block unlabelled deepfakes in less than three seconds. Any use of a person's voice or face in synthetic content requires their express consent. Five thousand accounts will be suspended under the Influencer Credential Rules (October 2025), which forbid unlicensed people from giving advice on law, education, health, or finance. For infractions, the Cyberspace Administration of China (CAC) suspends apps and levies fines of ¥100,000. Although the system is unparalleled in speed and scope, it is opaque, its removal criteria are not made public, and it is commonly used to suppress political dissent, satire, and whistleblowers. The government has final say because there is no independent appeal process and the state-controlled watermarking infrastructure raises surveillance concerns.

**Legal Response To Online Fake News In India**

1. **Defining Fake News:** The information that is fabricated to pass off as truth, with an intention to cause harm is “fake news”. It can be anything and everything-political propaganda, false health advisories or defamatory statements. Law related to 'fake news' often infringes on an issue such as defamation, or cybercrime, or public order, or consumer protection, etc. Because of the relative breadth and vagueness of the term, it is difficult to regulate fake news under a singular legislative clause.

2. **Constitutional Obligations and Legal Landscape in India:** Article 19(1)(a) of the Constitution of India grants its citizens the right of freedom of speech and expression. Article 19(2) permits the State to provide “reasonable restrictions” if the State deems the exercise of that right would harm public order, decency, defamation, and security of the State. Therefore, the Constitution provides the basis to restrict any false news depending on its content. Fake news is addressed indirectly by a number of legislative laws. Section 505 (statements causing public mischief), Section 295A (acts done to hurt religious feelings), and Section 153A (creating animosity between classes) are all covered under the Indian Penal Code. Section 499, which defines defamation and allows for action against people or organizations that spread false information, can also be helpful. Section 66D (cheating by personation by using computer resources) and Section 69A (blocking of websites) are two examples of provisions in the Information Technology Act of 2000 that address false content in the digital sphere

3. **Challenges in Enforcement:** Despite the presence of laws to curb the spread of fake news, the enforcement of it remains an uphill task! The fact the most fake news emerges anonymously and outside jurisdiction, and are then disseminated across India, makes their attribution and prosecution complex. Second, it demands a sharp mind and sophisticated judgment to distinguish between fake news and satire, opinion, or unverified reporting. This may not always be allowed by legal frameworks. Third, if fake news is overly criminalised, the institution of free press will start to crumble as the excessive oppressive laws will be used to punish journalists, activists, or political opponents.

4. **Judicial Response:** The negative effects of fake news and its rapid spread have been widely discussed by Indian courts. In Shreya Singhal v. Union of India (2015), the Supreme Court declared that Section 66A of the IT Act was unconstitutional and ambiguous, emphasizing the need for speech regulations to be both specific and appropriately tailored. In its ruling, the Supreme Court held that, even though preventing fake news is crucial, attempts to do so must pass the constitutional requirements of necessity and reasonableness and not restrict the right to free speech. This calls for a careful balancing act because, while fake news is bad, too much regulation could stifle journalism and free speech.

**Detailed Legal Provisions Addressing Online Fake News In India**

Section 153A of the Indian Penal Code (IPC) punishes inciting animosity between various groups based on factors such as religion, race, place of birth, residence, language, etc. It makes actions that harm public harmony illegal. The penalty can be a fine, three years in prison, or both. Section 295A: Addresses intentional and malevolent actions meant to offend religious sentiments by disparaging religion or religious convictions.

**Section 499 and 500:** Define and penalize criminal defamation, respectively. Section 500 prescribes punishment for defamation, which can be imprisonment up to 2 years, fine, or both.

**Section 505:** Relates to statements creating or promoting public mischief or fear, and false statements causing or likely to cause danger to public tranquillity. It carries punishment of imprisonment up to 3 years, or fine, or both.

**Bharatiya Nyaya Sanhita Act 2023:** Section 195(1)(d) imposes a maximum sentence of three years in prison, a fine, or both for creating or disseminating false or misleading information that compromises India's sovereignty, unity, integrity, or security.

**Information Technology Act, 2000 (IT Act) Section 66D:** Covers cheating by personation using computer resources, applicable when fake profiles or impersonation is used to spread misinformation. Punishable with imprisonment up to 3 years and fine.

**Section 69A:** Empowers the Central Government to direct blocking of public access to any information on the internet if it threatens the sovereignty, security of India, public order, or friendly relations with foreign states.

**Section 79:** Provides conditional immunity to intermediaries like social media platforms if they observe due diligence and remove or disable access to objectionable content when notified by authorities.

Information Technology (Digital Media Ethics Code and Intermediary Guidelines) Regulations, 2021: Require social media companies to have grievance redressal procedures and to promptly remove any identified false, misleading, or fake content. These regulations also give the government the authority to alert fact-checking organizations to fake news and mandate that intermediaries follow takedown instructions.

**Disaster Management Act, 2005 Section 54:** Penalizes false warnings or false information intended to cause panic or spread misinformation during disaster situations. Those circulating false alarms or information leading to panic face imprisonment and fines. However, the Act does not bar citizens from sharing genuine information or updates.

Representation of the People Act, 1951 Criminalises the dissemination of false information about a candidate or political party, with the intent of inducing or influencing the result of an election, with different maximum penalties of either imprisonment or fines. The law only prohibits misinformation that relates to election campaigns.

Provisional Bill - Prohibition of Fake News on social media Bill, 2023 The Bill proposes a Fake News Regulatory Authority established to investigate and respond to complaints on fake news. Section 3(1) prohibits the communication and contravention of communication of misinformation relating to public health, public safety, public tranquility, or the fairness of elections. The penalties include imprisonment for 2-5 years or directing the communication of fake news and up to 2 years for aiding or contravening. Special Courts are also proposed for expeditious trial, and courts can order platforms to publish retractions or no access or disable the material.

**Policy Recommendations**

- Legal Definition of Deepfakes: We need to determine any possible legal definitions in statute including a definition under the IT Act or DPDPA. Also, the difference between harmful and non harmful is also important to delineate.
- Criminalization of Malicious Use of Deepfakes: We need to create penal provisions for malicious creation or distribution of deepfakes without consent, especially for sexual or political deepfakes.
- Regulating Social Media Platforms: Ensure Social Media platforms watermark, trace origin, and develop capability to identify and flag AI-manipulated content.
- Develop a resource for regulating Synthetic Defamation Victims - Right to be forgotten:
- There should be a right to be forgotten for victims of synthetic Defamation or harassment.
- Digital literacy campaigns: Develop digital literacy campaigns where users will be educated about manipulated or edited content.
- Encouraging Ethical Development of AI: Through public and private policy development frameworks we could develop mechanisms to promote ethical transparency and accountability in the development of generative AI.
- Building Cyber Crime Unit Capacity in Forensic: Invest in training and equipment for cyber-crime units to ensure capacities to investigate and lay charges for AI based offences

**Conclusion**

Deepfakes and misinformation represent a new dimension of digital risk. They are dangerous because they can erode trust in institutions, create privacy violations, and destabilize democratic processes. While the Indian legal system currently provides some remedy, the existing laws are inadequate for a rapidly transitioning technology threatened by artificial intelligence. A multi stakeholder, multidisciplinary response is warranted. India's cyber laws

must change. It must acknowledge and treat synthetic media. It must define platform accountability to users and provide strong legal remedies to individuals. If these things do not change, informed dialogue and digital safety, as well as constitutional rights, may erode further in the information age. Factors such as requiring the plaintiff to assert a claim, a lack of precise definition related specifically to deepfakes, and the vague burden on technology platforms contribute to an inadequate forum. If substantive change must happen in a particular way in India, laws or regulations could be written that specifically address synthetic media.

There are several approaches that could be adopted to address the troubling deepfake challenge - watermarking the AI content as well as holding platforms accountable under an amended intermediary liability framework, or even a brand-new criminal offence if warranted. The Indian authorities have started to recognize deepfakes as a serious issue and have started to mobilize existing laws, but this has obvious problems, as demonstrated in the Rashmika Mandana case that underscores an urgent legal need and illustrates how severely delayed India's existing laws are. Offenders will look for and exploit loopholes, while either Parliament or regulators refuse to rectify these failures, all the while the victim will have to fight for justice. So, Parliament has much more to do. Precise definitions and consequences need to be established. There also needs to be some robust regulations that will impose concrete, proactive platform responsibilities to mitigate the for now harm of deepfakes on people and society in India.

**References**

References


1. Oxford English Dictionary. "Deepfake," accessed 2025.
2. Cambridge Dictionary. "Misinformation," accessed 2025.
3. Statutes and Legal Acts
4. Information Technology Act, 2000, Government of India. Relevant sections: 66E, 67, 67A, 69A.
5. Digital Personal Data Protection Act, 2023, Government of India.
6. Indian Penal Code, 1860, Government of India. Relevant sections: 499, 500, 419, 420, 463–469.
7. Representation of People Act, 1951, Government of India.
8. Disaster Management Act, 2005, Government of India.
9. Judicial Decisions
10. Supreme Court of India, Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., (2017) 10 SCC 1 (Right to Privacy).
11. Vaisakha & Ors. v. State of Rajasthan & Ors., AIR 1997 SC 3011 (Sexual Harassment Guidelines).
12. Shreya Singhal v. Union of India 2015 SC
13. Journal Articles
14. Jain, Abhay. "Deepfakes and Misinformation: Legal Remedies and Legislative Gaps,"
15. Indian Journal of Law, vol. 3, no. 2, Mar-Apr 2025, pp. 23-28. DOI: 10.36676/ijl.v3.i2.86.
16. International Legal Frameworks
17. European Union, Proposal for a Regulation on Artificial Intelligence (EU AI Act), 2024 (Draft).
18. People's Republic of China, Regulations on the Management of Deep Synthesis Internet Information Services, 2022.
19. United States, PROTECT Elections Act, 2023 (proposed).
20. Authoritative Websites and Reports
21. Ministry of Electronics and Information Technology (MEITY), Government of India. "India AI Strategy, 2024.
22. Standing Committee on Commerce, Government of India. "Review of the IPR Regime in India, 2024.
23. WACC Global. "Deepfakes, Cloned Voices, and Digital Media Literacy," August, 2025.
24. Chambers and Partners. "How India is Challenging Deepfakes," January, 2024.
25. JusCorpus Legal. "Can Spreading Fake News be Considered a Cybercrime Under Indian Law?" July, 2025.