Advanced International Journal for Research (AIJFR)
E-ISSN: 3048-7641 ● Website: www.aijfr.com ● Email: editor@aijfr.com

Deepfakes, Free Speech, and the Right to Truth: A Comparative Legal Study on Regulating Synthetic Media in the USA, UK, and India.

Devesh Kumar

Abstract

The rapid development of artificial intelligence has sparked the emergence of deepfakes, hyper-realistic synthetic media created using deep learning algorithms that can convincingly imitate human appearance and voice. While these tools offer creative and innovative possibilities, they also raise unprecedented legal, ethical, and social challenges. Deepfakes have been exploited for various malicious purposes, including non-consensual pornography, identity theft, political misinformation, financial fraud, and undermining public trust in media and democratic institutions. This paper provides a comparative legal analysis of how three major countries, the United States, the United Kingdom, and India, are addressing the regulatory challenges posed by deepfake technology. In the U.S., a fragmented legal system exists, with some federal legislation such as the *No Fakes Act* and the *Defiance Act*, along with diverse state laws targeting electoral manipulation and sexual privacy. The *UK's Online Safety Act 2023* is a significant step forward, criminalising the distribution of non-consensual explicit deepfake content. However, broader misuse remains covered by traditional laws like defamation, data protection, and harassment statutes. India, without a specific deepfake legislation, depends on provisions within the *Information Technology Act, 2000*, and the *Bharatiya Nyaya Sanhita, 2023*, which inadequately address the complex threats posed by synthetic media.

The paper further explores the central normative tension between the right to freedom of expression and the right to truth and protection from harm. It critically evaluates whether existing free speech doctrines are equipped to handle the unique challenges of synthetic falsification, concluding that while deepfakes pose novel technological risks, they do not create fundamentally new constitutional dilemmas. Rather, the regulation of deepfakes requires a strong extension of existing legal doctrines, with appropriate safeguards for satire, parody, and artistic freedom. Finally, the paper emphasises the growing threat that deepfakes pose to democratic discourse, particularly through their capacity to degrade informational trust, fuel the *Liar's dividend* and destabilise the evidentiary value of digital content. It calls for the development of harmonised legal standards, AI detection mechanisms, and ethical guidelines to safeguard individual dignity, ensure media authenticity, and strengthen democratic resilience in the digital age.

Keywords: Deepfakes, synthetic media, artificial intelligence, misinformation, digital disinformation, freedom of expression, right to truth, cyber law, non-consensual content, democratic integrity, media trust, USA, UK, India, *Online Safety Act 2023*, *Bharatiya Nyaya Sanhita 2023*, legal regulation, AI ethics, digital privacy, platform accountability.

1. Introduction

Artificial Intelligence (AI) has witnessed rapid and unprecedented growth in recent years, leading to remarkable technological advancements across various sectors. However, this progress has also given rise to concerning developments, one of the most notable being the emergence of DeepFake technology. DeepFakes involve the use of sophisticated AI algorithms to create highly realistic but fabricated audio-visual content that closely mimics genuine media. The ability of these synthetic creations to imitate real people and events with near-perfect accuracy has introduced a host of complex ethical, legal, and societal challenges. These range from concerns about misinformation, manipulation, and identity theft to broader implications for privacy, public trust, and democratic discourse. Recognising the potential dangers posed by such technology, particularly in terms of damaging personal reputations, spreading false narratives, and undermining public confidence in digital media, governments around the world are actively exploring legislative, regulatory, and technological measures to counteract the misuse of DeepFakes. Their efforts aim to establish accountability, safeguard citizens rights, and uphold the integrity of media and communication systems.

Deepfakes are a form of synthetic media generated using Artificial Intelligence (AI), wherein an individual's facial features, voice, or both are digitally superimposed onto another person's likeness. The term Deepfake is a blend of deep learning, a subset of AI responsible for generating these hyper-realistic imitations and the word fake, emphasising the deceptive nature of the content. These AI-generated simulations can replicate a person's appearance, speech, gestures, and mannerisms with striking accuracy, often making them nearly indistinguishable from genuine audio-visual material. While deepfake technology has potential applications in fields such as cinema, gaming, and education, its misuse raises significant concerns, and frequently, such media is produced without the consent of the individual being impersonated, violating their rights and personal dignity. The capacity of deepfakes to manipulate public perception, spread disinformation, defame individuals, particularly public figures and erode trust in authentic digital content has placed them at the forefront of ethical, legal, and social debates this is because with technological advancements making deepfake tools increasingly accessible and convincing, governments, regulatory bodies, and technology firms across the globe are now prioritizing the development of legal frameworks, detection mechanisms, and countermeasures to mitigate the harmful consequences of deepfake proliferation.

Although deepfakes are a relatively recent phenomenon in philosophical and ethical discourse, in terms of technological development, they are no longer novel. The term deepfake was coined in 2017 by a Reddit user with the same username, who employed existing machine learning tools, particularly deep learning based face swapping techniques, to insert the likenesses of female celebrities into pornographic videos without their consent. The term quickly gained traction and is now used more broadly to describe any synthetic media that uses artificial intelligence to manipulate audio, video, or images realistically. Despite the expansion of its meaning, the majority of deepfake content produced to date continues to involve non-consensual and coercive pornography, making it a serious concern in discussions of digital ethics, privacy rights, and gender-based online harm.

Different Types Of Deepfakes

Deepfake technology has developed at a rapid pace over the last decade, becoming increasingly accessible and sophisticated. Today, it broadly manifests itself in three major forms, each capable of significant misuse and causing trouble:

- **Face Swapping**

This technique involves replacing one individual's face with that of another in video or photographic content. It is often used to make it appear as though a person was present in a scene or participated in an event that never occurred.

- **Lip Syncing**

Lip syncing refers to manipulating footage to make it seem as though someone is saying something they never actually said. This technique is frequently used in audio-visual disinformation, especially in political or defamatory contexts.

- **Puppeteering (Puppet Technique)**

The puppet technique creates false movements or gestures by artificially animating a person's likeness. This often leads to unnatural body or facial movements being attributed to real individuals, making detection and interpretation more difficult.

Why deepfakes need to be regulated?

Deepfakes, once celebrated as a testament to the remarkable capabilities of artificial intelligence (AI), have increasingly become a pressing social concern due to their potential for misuse. While they demonstrate the sophistication of AI in producing highly realistic synthetic media, this very realism that makes them technologically impressive also introduces significant threats. These threats span sectors such as politics, journalism, law enforcement, and personal privacy. As the negative impacts of deepfakes become more evident, ranging from reputational damage and misinformation to threats against democratic processes and individual rights, governments and organisations worldwide have recognised the urgent need to establish effective regulations. The rising awareness of societal risks associated with deepfake technology has sparked a global conversation on ethical safeguards, legal accountability, and the development of detection tools to mitigate their harmful effects while allowing legitimate and creative uses of AI.

- **Psychological and Reputational Harm:**

The rise of deepfakes has caused serious psychological and reputational damage, especially for those targeted by non-consensual and malicious synthetic content. Victims often face long-term emotional and mental health problems resulting from unauthorised digital manipulation.

- **Non-consensual Explicit Content:**

Deepfake pornography, where a person's face is superimposed onto explicit content without their consent, is one of the most serious abuses of this technology. The effects are profoundly upsetting, which victims

describe feeling humiliated, anxious, depressed, and often suffer from post-traumatic stress. These fake materials are frequently shared widely online, increasing the harm through social shaming and loss of personal dignity. The highly realistic nature of such content makes it more damaging, as viewers may struggle to distinguish between real and fake images.

- **Reputational Damage:**

Beyond the psychological toll, deepfakes can cause lasting damage to a person's social and professional reputation. Specifically, public figures, influencers, and celebrities whose careers rely heavily on their image and trust are especially vulnerable. The spread of deepfake content, such as revenge porn or fabricated statements, can destroy credibility, lead to job loss, public backlash, and lasting stigma.

- **Undermining Democratic Processes:**

Deepfakes endanger the fundamental pillars of democratic society, specifically truth, accountability, and informed public discourse. As synthetic media grows more advanced and widely available, its capacity to alter political narratives and undermine institutions is becoming more apparent.

- **Election Interference:**

During election cycles, the risk of deepfakes being used to impersonate politicians or government officials is especially high. For example, synthetic videos may show candidates making offensive statements, endorsing false policies, or engaging in unethical behaviour. Such fabrications, even if exposed later, can influence voter opinions, change election results, and erode public confidence in democratic processes. The spread of deepfake technology in the age of misinformation contributes to a broader post-truth environment where objective facts are often replaced by emotionally convincing falsehoods. This loss of trust affects media outlets, public institutions, and democratic discussions. The global election cycle in 2024 has already increased concerns, with experts warning that AI-generated propaganda and synthetic campaign content could be weaponised to divide voters and undermine fair elections.

- **Economic and Financial Threats:**

Deepfakes have become a powerful tool in the arsenal of cybercriminals, enabling increasingly sophisticated forms of deception, fraud, and extortion. These attacks not only cause direct financial losses but also damage institutional trust and consumer confidence.

- **Fraud and Scams:**

One notable example involved a deepfake voice impersonation of a corporate executive, which resulted in a financial loss of $250,000. Criminals replicated the CEO's voice with such accuracy that subordinates were deceived into wiring funds under pretences. These kinds of impersonation-based frauds are on the rise and highlight the vulnerabilities of traditional verification systems.

- **Extortion and Blackmail:**

Malicious actors are using deepfakes to create compromising videos or images and threaten victims with exposure unless a ransom is paid. This type of digital extortion, powered by AI, is becoming harder to fight because the content looks real, even when it is completely fake.

- **Identity Theft and Biometric Fraud:**

Deepfakes are now used to bypass biometric authentication by mimicking facial and vocal patterns. This can grant unauthorised access to personal accounts, financial institutions, or government records. Manipulating such security systems presents a major challenge to cybersecurity and data protection frameworks.

- **Erosion of Trust in Media and Information Ecosystems:**

The rapid increase of deepfake content raises essential questions about the authenticity and reliability of information in the digital age. As AI-generated media becomes more realistic, it becomes more difficult for people to distinguish between truth and falsehood.

- **Dominance of Synthetic Content:**

Experts predict that in the coming years, a significant portion of online content may be artificially created. The growing gap between real and synthetic content presents major challenges for verifying information, journalism, and public awareness. As AI-generated media floods digital platforms, it erodes trust in genuine sources of information.

- **Amplification of Misinformation:**

Deepfakes have already been used to spread false narratives, manipulate consumer behaviour, and incite social unrest. For example, fabricated videos showing influential figures endorsing products, expressing extreme opinions, or inciting violence can distort public perception and provoke reactive behaviour. Such misuse greatly amplifies the spread of misinformation and undermines social stability.

- **Legitimacy and Content Certification Concerns:**

Efforts to combat deepfake threats have led to proposals for certifying authentic content, such as through cryptographic watermarking or provenance tracking. For example, the U.S. Executive Order on AI includes provisions for developing technical standards to distinguish verified media from AI-generated fabrications. However, this approach risks creating a fragmented information environment where content is either certified or not, which could deepen public mistrust and complicate content governance.

Comparative Legal Approaches to Deepfakes: The Usa, Uk, And India

The legal response to deepfake technology varies greatly across different jurisdictions, shaped by each country's legal systems, cultural norms, and technological progress. While some nations have enacted specialised laws to address deepfake misuse, others depend on adapting existing legal frameworks to confront the challenges of this new and rapidly changing technology. As deepfake abilities improve and their misuse spreads, the need for international cooperation and standardised regulation becomes more urgent.

- **United States**

Federal Legislation

Currently, the United States does not have a comprehensive federal statute specifically targeting deepfake content. However, growing recognition of the risks posed by AI-generated synthetic media has led to several legislative proposals aimed at closing this regulatory gap. One such initiative is *the No Artificial Intelligence Fake Replicas and Unauthorised Duplications (No AI FRAUD) Act* , which seeks to criminalise the unauthorised creation of deepfake representations, visual or auditory, of real individuals, whether living or deceased. This proposed legislation underscores the growing complexity of AI-generated content and the urgent need to address impersonation across visual and vocal dimensions.

Other legislative efforts include:

- **The *NO FAKES Act (Nurture Originals, Foster Art, and Keep Entertainment Safe Act)***: Aims to protect performer's voices and likenesses from unauthorised AI-generated copying.
- The *DEFIANCE Act (Disrupt Explicit Forged Images and Non-Consensual Edits Act):* Aims to protect individuals from creating and distributing deepfake pornography and other non-consensual explicit materials.

Despite these proposals, a unified and enforceable federal framework for deepfake regulation remains absent, resulting in fragmented protection.

State-Level Legislation:

Several U.S. states have passed separate laws to address particular threats from deepfakes, especially related to elections, sexual privacy, and identity theft.

- California**:**
  - *Assembly Bill 730* prohibits distributing deceptive deepfake content meant to sway political elections within 60 days of the vote.
  - *Assembly Bill 602 en*ables civil lawsuits against individuals who produce or distribute deepfake pornography without consent, giving victims the ability to seek justice.
- Texas**:**
  - *Senate Bill 751* criminalises the creation and distribution of deepfakes intended to deceive voters or influence election results. It also targets non-consensual sexually explicit deepfake content.

Other states, including *New York, Florida, Virginia, and Illinois***,** have introduced or enacted legislation targeting aspects of deepfake misuse. However, the lack of uniformity in definitions, scope, and penalties across states has created a patchwork of protections rather than a cohesive national policy.

- **United Kingdom**

The United Kingdom has taken a significant step by enacting the Online Safety Act 2023, which criminalises the sharing of deepfake sexually explicit images when the intent is to cause distress or when the perpetrator is recklessly indifferent to the consequences. This law marks a progressive move in addressing the harms caused by non-consensual synthetic media. The main goal of the Online Safety Act (OSA) is to improve online safety for both children and adults by imposing specific obligations on social media platforms and search engines, requiring them to take active measures to protect users.

Nevertheless, victims of other forms of deepfake abuse, such as defamation, identity manipulation, or political misinformation, must still rely on pre-existing legal avenues, such as:

1. Defamation law
2. Harassment legislation
3. Data protection regulations under the UK GDPR

These existing laws, while useful in some contexts, are not always well-suited to handle the unique and evolving challenges presented by AI-generated media. This highlights the need for further legal reform tailored specifically to the deepfake phenomenon, especially concerning its impact on free speech, digital identity, and public trust. However, the Online Safety Act (OSA) is an extensive and intricate piece of legislation, comprising 241 sections and 17 schedules. It addresses a wide range of illegal content and online activities, while introducing significant new responsibilities for digital platforms and the communications regulator, Ofcom. The Act has also sparked considerable controversy, having undergone intense public and parliamentary debate before receiving Royal Assent. Critics have expressed concern that, in striving to enhance online safety, the legislation could curtail freedom of expression, compromise internet security, and prove highly divisive in its broader societal impact.

- **INDIA**

Currently, India does not have a dedicated statute specifically tailored to regulate deepfake technology. While certain provisions under the ***I****nformation Technology Act, 2000* and the newly enacted *Bharatiya Nyaya Sanhita, 2023 (BNS)* cover aspects of cybercrime, they are not sufficient to comprehensively address the multifaceted legal challenges posed by AI-generated deepfakes.

Relevant Existing Legal Provisions:

Information Technology Act 2000

- Section 66D: Penalises cheating through personation using computer resources in cases of identity fraud via deepfake impersonation.
- Section 67: Criminalises the publishing or transmission of obscene material in electronic form, commonly used in cases involving deepfake pornography.

Bharatiya Nyaya Sanhita, 2023 (BNS)

- Section 73 *(corresponding to IPC Section 500)*: Penalises criminal defamation, which applies when deepfakes are used to damage a person's reputation.
- Section 78 *(replaces IPC Section 509)*: Addresses insult to the modesty of a woman, which may be relevant when deepfakes are used to produce non-consensual sexual content.
- Section 83 *(partially corresponds to IPC Section 468/471)*: Covers forgery intended to harm reputation or cheating, which can be extended to the creation and dissemination of deepfake content.
- Section 336: Punishes cheating by impersonation through electronic or digital means, which directly aligns with how deepfakes are created and used.

These provisions provide a fragmented framework for penalising specific harms caused by deepfakes, such as identity fraud, obscenity, defamation, and impersonation. However, the absence of a unified, technologically updated law that specifically defines and regulates deepfakes as a distinct category leaves significant gaps in enforcement, prevention, and redressal. Given the rapidly evolving nature of synthetic media and its potential for misuse, ranging from political manipulation and financial fraud to severe violations of privacy, there is an urgent call for comprehensive legal reform. This could involve enacting a dedicated AI and Synthetic Media Regulation Law that clearly defines deepfakes, criminalises non-consensual uses, outlines exceptions for satire or legitimate artistic expression, and integrates digital forensics and detection protocols.

The Central Conflict: Free Speech Vs. Truth and Harm

The regulation of deepfakes raises essential constitutional and philosophical questions: *Does limiting deepfake content violate the principles of freedom of expression?* This issue becomes especially urgent as evidence grows that certain uses of deepfakes, particularly those that are malicious, deceptive, or defamatory, threaten individuals and democratic institutions. While automated detection tools and regulatory actions might seem like practical solutions, their compatibility with freedom of expression rights requires careful consideration. Two overly simple responses are often proposed and quickly dismissed. The first argues that deepfakes are automatically not protected by free speech laws just because they are fabricated. This view overlooks that not all false content lacks expressive value. Satire, parody, and artistic fiction often use fabricated elements while adding to public dialogue. The second claims that deepfakes should only be regulated if falsely presented as real**,** ignoring that even harmless synthetic media can cause serious indirect harm.

To assess the legitimacy of regulating deepfakes within a democratic framework, it is essential first to revisit the foundational rationale for protecting freedom of expression. This right fulfils vital democratic functions, including enabling political discourse, promoting the pursuit of truth, safeguarding individual autonomy, and holding those in power accountable. Nonetheless, these values do not necessitate absolute freedom; legal regulations concerning defamation, obscenity, incitement, and deceptive advertising delineate the permissible boundaries of speech, balancing expressive rights with other societal interests. When applying this framework to deepfakes, the pivotal question is not solely whether they pose novel

threats, an affirmation supported by their potential to cause harm or whether regulatory measures might restrict expressive freedoms, an inevitable consequence, but whether such restrictions invoke unique or unprecedented challenges to freedom of expression.

Notably, the evidence suggests that the answer is no. Although regulating deepfakes involves intricate legal and practical issues, the fundamental constitutional questions largely mirror longstanding concerns associated with restrictions on harmful or deceptive speech in other contexts. Therefore, the advent of deepfake technology does not require the creation of entirely new free speech doctrines, but instead calls for a nuanced application of existing principles to a technologically advanced context. As such, any regulatory strategy must continue to distinguish between protected and unprotected speech, ensure proportionality, and leave room for legitimate expression, including satire, parody, and political dissent.

When we consider the U.S. system of free speech, it's clear that the justifications for protecting this fundamental right are deeply linked with libertarian interpretations of Enlightenment ideals. These ideas emphasise the pursuit of truth and honour the rationality inherent in each person as the famous thinker John Milton vividly expressed this when he stated, '*Where there is a strong desire to learn, there will inevitably be lively debates, extensive writings, and numerous opinions; for the opinions of virtuous individuals are merely knowledge in the process of formation.*' This lively exchange of thoughts and ideas highlights the importance of free expression in promoting personal growth and societal progress.

While deepfakes and other forms of synthetic media are often employed for harmless or creative purposes, they are increasingly viewed as a significant and evolving threat to democratic governance. A well-functioning democracy relies fundamentally on the availability of accurate and trustworthy public information. In recent years, audio and video recordings have emerged as critical components of this information ecosystem, serving as persuasive and seemingly objective sources of evidence. However, this trust is severely compromised when synthetic media becomes so sophisticated that it becomes virtually indistinguishable from authentic content.

The central concern is that as deepfakes become more *realistic*, *easily produced*, *resistant to detection*, and *widely disseminated*, even *genuine audio-visual material* may lose its evidentiary value and credibility. This phenomenon gives rise to a dangerous consequence known as the 'Liar's dividend' , a situation in which individuals caught in authentic recordings can falsely claim the material is fabricated, thus escaping accountability. Conversely, falsehoods masquerading as truth can go undetected, leading to public manipulation and confusion. This degradation of informational trust offers a powerful tool for those seeking to destabilise democratic institutions, delegitimise opposition voices, and erode public confidence in media and governance.

Political technology advisor Nina Schick has aptly described deepfakes as the latest evolving threat in an increasingly dangerous and untrustworthy information ecosystem, highlighting their capacity to disrupt democratic discourse and decision-making. As deepfake technology continues to advance, addressing its implications for democratic societies has become an urgent imperative. Effective responses must involve not only technological detection tools but also legal, ethical, and institutional safeguards that reinforce the integrity of information upon which democratic participation depends.

Conclusion

While deepfake technology offers many benefits, its advanced capabilities mean that many fake videos and images are often indistinguishable from real ones. Its ability to mimic human behaviour and appearances enables the creation of convincing counterfeit content, which can spread misinformation and falsehoods. Without clear regulations, the malicious use of deepfakes can cause serious and long-lasting damage. Currently, social media platforms independently decide what content to allow or remove. For example, there have been recent cases of deepfake images of Taylor Swift circulating online. The U.S. government has recognised that these platforms have a responsibility to limit the spread of fake and non-consensual content. Legal options like libel lawsuits could be considered, but issues of accountability remain, whether it falls on the platform or the individual creator. In the recent case of images on X (formerly Twitter), the platform quickly took down the deepfakes and confirmed they were fakes.

Legislation currently helps address some issues related to malicious deepfake use, but there is an urgent need for detailed rules that protect individual privacy and identity, while also respecting free speech rights. Deepfakes can dangerously blur the line between reality and fiction, and without proper regulation, they could be exploited for harmful purposes. This highlights the necessity for comprehensive laws covering all aspects of deepfake technology, including misuse and its consequences. For instance, China's Deep Synthesis Technology Regulation demonstrates a strict approach to managing this problem, with severe penalties for abuse. But the challenge goes beyond legal measures, raising important ethical questions. Proper regulation can help rebuild trust in media, enhance security at both national and international levels, and create a safer online space, ultimately preserving human dignity.

References

1. Gollerkeri, G. (n.d.). Digital misinformation: How deepfakes empower the "liar's dividend" in a post-truth era. Deccan Herald. https://www.deccanherald.com/opinion/deepfakes-and-the-liars-dividend-3497282
2. Ramluckan, T. (2024). Deepfakes: The legal implications. International Conference on Cyber Warfare and Security, 19(1), 282–288. https://doi.org/10.34190/iccws.19.1.2099
3. What is Artificial Intelligence? definition, uses, and types. Coursera. (n.d.). https://www.coursera.org/articles/what-is-artificial-intelligence
4. Miller, D., Somoray, K., & Stevens, H. (2025). A Shallow History of Deepfakes. https://doi.org/10.2139/ssrn.5130379
5. Barber, A. (2023). Freedom of expression meets deepfakes. Synthese, 202(2). https://doi.org/10.1007/s11229-023-04266-4
6. Semanticscholar. (n.d.-az). https://pdfs.semanticscholar.org/6f93/5d299c7f4f76fad19c5be3c2219e4bef921c.pdf
7. AI-Powered Research Tool. Semantic Scholar. (n.d.). https://www.semanticscholar.org/
8. Damiani, J. (2024, February 20). A voice deepfake was used to scam a CEO out of $243,000. Forbes. https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/

9. Chen, H., & Magramo, K. (2024, February 4). Finance worker pays out $25 million after video call with Deepfake "chief financial officer." CNN. https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk
10. The US is drafting new laws to protect against AI-generated deepfakes. World Economic Forum. (n.d.-a). https://www.weforum.org/stories/2024/02/ai-deepfakes-legislation-trust/
11. Schroeder, Jared. "Free Expression Rationales and the Problem of Deepfakes within the E.U. and U.S. Legal Systems." SSRN Electronic Journal, 2019, doi:10.2139/ssrn.3503617.
12. Salazar introduces the No Ai Fraud Act. Representative Maria Salazar. (2024, January 10). https://salazar.house.gov/media/press-releases/salazar-introduces-no-ai-fraud-act
13. No Ai Fraud Act is a significant step for right of publicity. (n.d.-ab). https://www.honigman.com/media/publication/3216_Law360%20-%20No%20AI%20FRAUD%20Act%20Is%20A%20Significant%20Step%20For%20Right%20Of%20Publicity.pdf
14. Akin, an elite global law firm. Akin Gump Strauss Hauer & Feld LLP - California Deepfake Laws First in Country to Take Effect. (n.d.). https://www.akingump.com/en/insights/blogs/ag-data-dive/california-deepfake-laws-first-in-country-to-take-effect
15. Greggwirth. (2024, June 27). Deepfakes: Federal and state regulation aims to curb a growing threat. Thomson Reuters Institute. https://www.thomsonreuters.com/en-us/posts/government/deepfakes-federal-state-regulation/
16. Online safety act: Explainer. GOV.UK. (n.d.-a). https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer
17. Vallance, I. R.-J. & C. (2023, October 26). Online safety bill: Divisive internet rules become law. BBC News. https://www.bbc.com/news/technology-67221691
18. Information technology act, 2000. (n.d.-y). https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf
19. the Bharatiya Nyaya Sanhita, 2023. (n.d.-a). https://www.indiacode.nic.in/bitstream/123456789/20062/1/a2023-45.pdf
20. Bhale, S. (2025). Deepfake Laws in India: The Need for Legal Regulation in the AI Era. https://doi.org/10.2139/ssrn.5153296
21. Barber, A. (2023a). Freedom of expression meets deepfakes. Synthese, 202(2). https://doi.org/10.1007/s11229-023-04266-4
22. Schroeder, J. (2019). Free expression rationales and the problem of deepfakes within the E.U. and U.S. Legal Systems. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3503617
23. Gollerkeri, G. (n.d.). Digital misinformation: How deepfakes empower the "liar's dividend" in a post-truth era. Deccan Herald. https://www.deccanherald.com/opinion/deepfakes-and-the-liars-dividend-3497282
24. Schick, N. (2020). Deep fakes and the Infocalypse: What you urgently need to know. Conran Octopus.