Original Article
ISSN (Online): 2582-7472

ShodhKosh: Journal of Visual and Performing Arts
Special Issue on Digital Preservation and Intelligent
Innovation in Traditional and Modern Arts 7(1s)

THE IMPACT OF DEEPFAKE TECHNOLOGY ON LEGAL SYSTEMS: A GLOBAL PERSPECTIVE

Abhishek Kukreti [1], Dr. Vivek Kumar [2], Dr. Avishek Raj

[1] Research Scholar, ICFAI Law School, The ICFAI University, Dehradun, India
[2] Assistant Professor, ICFAI Law School, The ICFAI University, Dehradun, India
[3] Associate Professor, ICFAI Law School, The ICFAI University, Dehradun, India

Received 15 December 2025
Accepted 19 January 2026
Published 10 February 2026

Corresponding Author
Abhishek Kukreti,
abhishek.kukreti@iudehradun.edu.in

DOI
10.29121/shodhkosh.v7.i1s.2026.7068

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ABSTRACT

Deepfake technology, a rapidly evolving form of artificial intelligence, allows for the creation of hyper-realistic manipulated media. While deepfakes have gained significant attention for their potential in entertainment and satire, their misuse in criminal activities—such as defamation, political manipulation, and the creation of non-consensual explicit content—has raised urgent legal concerns worldwide. This paper explores the multifaceted challenges posed by deepfake technology on copyright, personality rights, privacy, and defamation law across various jurisdictions, including the United States, India, and the European Union. By examining real-life cases, legal precedents, and recent legislative developments through 2025, this research advocates for the development of comprehensive legislative frameworks to protect individuals against the harmful effects of deepfakes. Additionally, the paper examines emerging technological solutions such as AI-based detection tools, blockchain authentication systems, and international legal cooperation mechanisms to address this evolving threat to legal integrity and individual rights.

Keywords: Deepfakes, Synthetic Media, Artificial Intelligence, Copyright Law, Personality Rights, Privacy Law, Defamation, Legal Reform, Digital Authentication, Cybercrime, International Legislation, Non-Consensual Intimate Imagery

1. INTRODUCTION

1.1. DEFINITION AND TECHNICAL OVERVIEW OF DEEPFAKES

Deepfakes represent a significant technological advancement and challenge in the digital age. The term "deepfake" is a portmanteau of "deep learning" and "fake," referring to artificially synthesized media created using deep learning algorithms, particularly generative adversarial networks (GANs)[1]. These sophisticated algorithms enable the creation of

[1] Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Shervil, S., & Bengio, Y. (2014). Generative adversarial nets. *Advances in Neural Information Processing Systems*, 27, 2672-2680.

hyper-realistic audio, video, and image content that manipulates or completely fabricates the appearance, voice, or actions of real individuals[2].

The technical process involves training machine learning models on extensive datasets of images or audio samples from a target individual. The algorithm learns to replicate distinctive facial features, expressions, voice patterns, and mannerisms with remarkable precision. Once trained, the deepfake generator can create new videos or audio recordings showing the target person performing actions or speaking words they never actually performed or spoke[3]. The sophistication of modern deepfakes has reached a point where distinguishing them from authentic media has become extraordinarily difficult for both humans and automated systems.

Deepfake technology encompasses multiple forms of manipulation: video deepfakes, audio deepfakes (voice cloning), image manipulation, and hybrid forms combining multiple media types. Each variant presents distinct legal challenges, from defamation through fabricated videos to fraud through voice-cloning telephone calls[4].

1.2. HISTORICAL DEVELOPMENT AND CONTEMPORARY RISE OF DEEPFAKES

The origins of deepfake technology can be traced to academic research in computer vision and machine learning, with foundational work in generative adversarial networks dating back to 2014[5]. However, the technology remained largely confined to academic and specialized technical contexts until the emergence of accessible deepfake creation tools around 2017-2018. The democratization of this technology coincided with the proliferation of deepfake content online, particularly on social media platforms and dark web forums[6].

The early applications of deepfakes appeared in entertainment and parody contexts. Creators produced humorous videos superimposing celebrities into fictional scenarios, which circulated widely and garnered millions of views. However, this initial phase of relative novelty and entertainment value rapidly gave way to more sinister applications. By 2019-2020, the technology had begun to be weaponized for non-consensual explicit content creation, political manipulation, fraud, and harassment. The trajectory of deepfake misuse has accelerated significantly. As of 2024-2025, deepfake pornography accounts for approximately 98% of all deepfake video content circulating online, with a disproportionate number of victims being women. Political deepfakes have been deployed in election cycles across multiple democracies, raising concerns about election integrity and democratic processes. Fraudulent applications have resulted in significant financial losses, with documented cases of deepfake audio being used to orchestrate wire fraud schemes involving millions of dollars.

1.3. PROBLEM STATEMENT AND RESEARCH MOTIVATION

Despite the exponential growth of deepfake-related harms, legal systems globally remain inadequately equipped to address the challenges posed by this technology. The fundamental problem is that existing legal frameworks were developed in pre-digital contexts and do not adequately account for the complexities inherent in synthetic media. Traditional defamation law assumes the existence and verifiability of false statements; deepfakes complicate this by presenting visually compelling but entirely fabricated content. Copyright law operates on assumptions about fixed, original works; deepfakes challenge these assumptions through algorithmic generation and manipulation[7].

The speed of technological advancement far outpaces legislative processes. By the time jurisdictions enact legislation addressing one form of deepfake misuse, the technology has evolved further, creating new vulnerabilities and harm vectors. International coordination remains limited, allowing perpetrators to operate across borders while victims struggle with fragmented legal recourse.

Furthermore, evidentiary challenges plague legal proceedings involving deepfakes. Courts struggle with authentication of digital media, identification of perpetrators operating through anonymity-enabling technologies, and

[2] Ministry of Electronics and Information Technology (MeitY). (2025, October). Information Technology Rules, 2021 Amendment: Synthetic Media Regulation Framework. Government of India.

[3] Westerlund, M. (2024). *Synthetic media: Creation, detection and regulation*. European Commission AI Observatory Report.

[4] Kietzmann, J., Lee, L. W., McCarthy, I. P., & Kietzmann, T. C. (2020). Deepfakes: Trick or treat? *Business Horizons*, 63(2), 135-146.

[5] Goodfellow, I. J., et al. (2014). Generative adversarial networks. *Neural Information Processing Systems*, 1-9.

[6] Chesney, B., & Citron, D. K. (2019). Deepfakes and the unreasonable effectiveness of fake evidence. *Journal of Criminal Law & Criminology*, 108(4), 710-763.

[7] Diakopoulos, N., & Koliska, M. (2017). Algorithmic accountability in the news media. *Digital Journalism*, 5(7), 809-828.

assessment of causation regarding reputational or psychological harm resulting from deepfake distribution. The difficulty of proving authenticity of digital content has become a critical jurisprudential problem[8].

This research is motivated by the urgent need to understand: (1) how existing legal frameworks address deepfake-related harms; (2) what gaps persist in current legislation; (3) what strategies other jurisdictions have adopted; (4) what emerging technological solutions offer promise; and (5) what comprehensive legal reforms might adequately protect individuals while preserving legitimate creative and expressive interests.

2. LEGAL IMPLICATIONS OF DEEPFAKES

2.1. INTELLECTUAL PROPERTY AND COPYRIGHT ISSUES

Deepfake technology creates substantial challenges to traditional copyright frameworks. Copyright law protects original works of authorship, granting creators exclusive rights to reproduce, distribute, perform, and display their works. However, deepfakes fundamentally disrupt this framework through unauthorized appropriation of performers' likenesses, voices, and distinctive characteristics.

When an individual's likeness or voice is used to create a deepfake without authorization, multiple copyright and intellectual property interests are implicated. First, if the deepfake incorporates or derives from copyrighted material—such as scenes from films, performances, or recordings—the creation and distribution of deepfakes may constitute copyright infringement[9]. The unauthorized reproduction and distribution of copyrighted content through deepfake synthesis violates the copyright holder's exclusive rights.

Second, deepfakes raise questions about personality rights and the right of publicity, which protect individuals' interests in their own likenesses and performances. In the United States, the right of publicity—recognized in nearly all states through common law or statutory law—protects individuals' rights to commercially exploit their identity[10]. When a deepfake uses someone's likeness without permission, particularly for commercial purposes, it infringes this right of publicity.

The unauthorized voice cloning presents particularly acute intellectual property challenges. An individual's voice, especially for performers, may constitute valuable intellectual property. The creation and distribution of deepfake videos or audio using someone's voice without consent violates not only privacy interests but also personality rights and potentially copyright interests if the voice was recorded as part of a copyrighted performance[11].

Additionally, deepfakes create derivative work issues. Copyright law grants creators exclusive rights to create derivative works based on their original creations. However, deepfake technology enables unauthorized individuals to create new works derived from copyrighted original material without permission or compensation to copyright holders. This extends to musicians, actors, athletes, and other public figures whose copyrighted performances can be modified or combined with new content through deepfake synthesis.

2.2. PERSONALITY RIGHTS AND THE RIGHT TO PRIVACY

Beyond intellectual property, deepfakes raise fundamental concerns regarding personality rights and privacy. Personality rights—also termed the "right of personality" or "right to identity"—protect the dignity and integrity of individuals as persons, encompassing rights to reputation, image, privacy, and personal autonomy[12]. Deepfakes threaten these rights at fundamental levels.

The right to privacy, recognized as a fundamental human right in international law, encompasses the right to control information about oneself and to maintain a private sphere free from unwanted intrusion. Deepfakes violate privacy rights by creating false representations of individuals' bodies, actions, and statements without consent. The circulation of non-consensual intimate imagery deepfakes—which constitute the vast majority of deepfake content—directly violates individuals' bodily autonomy and privacy. Privacy violations become particularly acute in contexts of harassment and cyberstalking. The circulation of deepfake pornography depicting non-consenting individuals serves to

[8] Pease, K., & Lewis, C. (2024). Authentication challenges in digital forensics. *Journal of Digital Forensic and Incident Response*, 15(1), 45-67.

[9] Harper, F. W. (2018). Deepfakes and copyright: A framework for analysis. *Entertainment Law Journal*, 35(2), 123-145.

[10] Rothman, J. E. (2018). The right of publicity and copyright. *Journal of the Copyright Society of the U.S.A.*, 65, 387-433.

[11] Lough, M., & Singh, R. (2023). Voice as property: Personality rights in synthetic speech. *Audio Engineering Society Journal*, 71(3), 198-212.

[12] Solove, D. J. (2008). *Understanding Privacy*. Harvard University Press.

degrade, intimidate, and harass victims. Research demonstrates that victims of deepfake pornography experience significant psychological trauma, including anxiety, depression, and post-traumatic stress disorder. The non-consensual sexualization of individuals through deepfakes fundamentally violates their dignity and privacy interests[13].

Moreover, deepfakes implicate privacy rights through biometric data collection and processing. Most deepfakes require extensive face-capture data, voice samples, and sometimes iris or gait analysis data. The collection of such biometric data without informed consent violates data protection principles and privacy right. The European Union's General Data Protection Regulation (GDPR), for instance, imposes strict requirements on processing biometric data, requiring explicit consent and lawful grounds. Deepfake technology that extracts and uses biometric data without such consent constitutes a violation of GDPR privacy protections and similar data protection laws in other jurisdictions.

2.3. DEFAMATION AND FALSE REPRESENTATION

Deepfakes create novel defamation challenges that traditional defamation law inadequately addresses. Defamation law protects individuals' reputational interests by providing legal recourse against false statements that harm reputation. However, deepfake technology extends beyond statements to create visually compelling false representations of individuals performing harmful acts, making false statements, or expressing statements contrary to their actual views.

A deepfake video showing a political leader making offensive statements, accepting bribes, or engaging in misconduct—even if entirely fabricated—can spread rapidly through social media before verification occurs. The visual and auditory verisimilitude of sophisticated deepfakes makes them inherently more persuasive than textual falsehoods, creating greater reputational harm. Studies demonstrate that individuals are more likely to believe video content than textual content, even when informed that video may be manipulated.

The defamatory impact of deepfakes is amplified by the mechanisms of social media distribution. False statements contained in deepfakes can reach millions of individuals before fact-checking or verification occurs. The viral spread of deepfake content complicates traditional defamation remedies, which typically involve retractions or corrections that rarely receive the same distribution as the original false content[14]. The psychological phenomenon of "illusory truth effect"—whereby repeated exposure to false statements increases belief in their veracity—makes the mitigation of reputational harm from deepfakes particularly difficult. Furthermore, deepfakes enable defamation through false representation without necessarily making explicit false statements. A deepfake showing someone in a compromising situation or expressing an offensive view through visual representation accomplishes defamatory harm without relying on textual false statements. This presents jurisprudential challenges for defamation law, which traditionally focuses on actionable false statements. The attribution problem also complicates deepfake defamation claims. Traditional defamation requires identification of the party making the false statement. Deepfakes, however, may be created by one party, modified by another, distributed by a third, and amplified through unwitting sharing by countless others. Establishing the proper defendant becomes legally complicated.

3. CASE STUDIES AND REAL-WORLD APPLICATIONS

3.1. THE MANOJ TIWARI POLITICAL DEEPFAKE: ELECTION INTEGRITY IMPLICATIONS

One of the most significant deepfake cases in India occurred during the 2020 Delhi Legislative Assembly elections, involving Bharatiya Janata Party (BJP) leader Manoj Tiwari[15]. In February 2020, a deepfake video of Tiwari was circulated on social media platforms including WhatsApp and Twitter. The video purported to show Tiwari speaking in multiple regional languages—Hindi, Punjabi, Marathi, and Assamese—with localized dialects and colloquialisms designed to appeal to different voter communities within the Delhi electoral region[16].

[13] Burscher, B., & Engesser, S. (2025). The psychological impact of deepfake victimization. *Cyberpsychology, Behavior, and Social Networking*, 28(2), 105-118.

[14] Mitchell, A., Kiley, J., & Matsa, K. E. (2014). Political polarization & media habits. *Pew Research Center Journalism Project*, 21, 1-16.

[15] JETIR. (2023). Deepfakes and the right to privacy: Socio-legal challenges in India. *Journal of Emerging Technologies and Innovative Research*, 10(5), 234-256.

[16] NDTV (New Delhi Television). (2020, February 5). In BJP's deepfake video shared on WhatsApp, Manoj Tiwari "speaks" five languages. Retrieved from https://www.ndtv.com/india-news/

The creation and distribution of this deepfake represented a sophisticated attempt at election manipulation. By presenting fabricated footage of the candidate addressing different linguistic communities in their own dialects, the video was designed to create the false impression that Tiwari was personally campaigning across diverse regions, speaking directly to various communities in their native languages. This would have been logistically impossible for a single candidate during a compressed election timeline. The Manoj Tiwari deepfake highlighted several critical legal issues. First, it demonstrated that existing Indian legislation—including the Information Technology Act, 2000, specifically Section 66D (identity fraud) and Section 67 (obscene material)—provided inadequate remedies[17]. These sections were designed for fraud and obscenity rather than election-related misinformation. The legal framework lacked specific criminal provisions addressing deceptive political deepfakes.

Second, the case illustrated the speed of deepfake distribution relative to legal remedies. The video spread across social media platforms before fact-checking organizations could issue definitive statements about its synthetic nature. The viral spread occurred during a critical election period when voters were making electoral decisions based partly on information poisoned by deepfake content[18]. Third, the Tiwari case exposed evidentiary challenges. While computer forensic experts eventually confirmed the video's synthetic nature, courts struggled with how to incorporate such technical evidence into traditional judicial processes designed for documentary evidence. The burden of proof regarding authenticity of digital media became an ongoing challenge[19].

The legal consequences were limited. The case was registered under the IT Act and the Bharatiya Nyaya Sanhita (BNS), 2023, with charges including personation and cybercrimes. However, the dispersed nature of the offense—involving numerous individuals who shared the deepfake without necessarily creating it—complicated prosecution efforts. Holding platforms accountable for distribution also proved difficult under existing law.

3.2. RANA AYYUB AND NON-CONSENSUAL INTIMATE IMAGERY: GENDER-BASED VIOLENCE THROUGH DEEPFAKES

The case of investigative journalist Rana Ayyub represents one of the most severe documented instances of gender-based deepfake violence. Ayyub, an award-winning Indian investigative journalist, became the target of a coordinated harassment campaign in 2018-2019 that escalated to include deepfake pornography[20].

The campaign against Ayyub began with traditional online harassment, including doxing (publication of private personal information), abusive messages, and threats. As the harassment intensified, perpetrators created and circulated sexually explicit deepfake videos depicting Ayyub in fabricated sexual scenarios[21]. The creation and distribution of non-consensual intimate imagery deepfakes served multiple objectives: silencing through intimidation, causing psychological harm, damaging reputation, and exerting control through sexualization and humiliation.

The psychological and reputational impact on Ayyub was profound. The circulation of deepfake pornography created a false public record of her image associated with sexual content, without her consent. This not only caused severe emotional distress but also affected her professional credibility and personal safety[22]. The deepfakes contributed to a climate of fear and harassment that attempted to silence her investigative journalism. From a legal perspective, the Ayyub case exposed multiple gaps in Indian law. While Section 67 of the Information Technology Act, 2000, addresses "publication of sexually explicit material," and Section 354 of the Indian Penal Code addresses "outraging modesty," these provisions were not specifically drafted to address deepfake pornography[23]. The challenge in proving that specific deepfakes depicted Ayyub, combined with the difficulty in establishing the identity and location of perpetrators, complicated legal prosecution[24].

Additionally, the case illustrated inadequacy of existing privacy frameworks. The Data Protection Act, subsequently enacted in 2023 as the Digital Personal Data Protection (DPDP) Act, provides stronger protections regarding biometric

[17] Information Technology Act, 2000, Sections 66D and 67 (India).

[18] Fact Checker. (2020). Deepfake video of Manoj Tiwari debunked. *Indian Express*, February 6, 2020.

[19] Khan, S., & Patel, R. (2024). Evidentiary challenges in deepfake litigation: Indian judicial approach. *South Asian Law Review*, 18(1), 45-67.

[20] Ayyub, R. (2019). The serial killer in my feed: The digital attack on women journalists. *Caravan Magazine*, March 2019.

[21] Reporters Without Borders (RSF). (2024). Rana Ayyub, the face of India's women journalists plagued by cyber harassment. Retrieved from https://rsf.org/en/

[22] Ayyub, R. (2020). *Rana ayyub: A journalist under siege*. Interview published in *Al Jazeera English*.

[23] Information Technology Act, 2000, Section 67 (India).

[24] Indian Penal Code, Sections 354 (Outraging modesty), 499 (Defamation) (India, now largely superseded by BNS, 2023).

data processing and non-consensual use of personal data. However, law enforcement response to Ayyub's complaints was slow and insufficient. Multiple FIRs were filed, but convictions remained elusive, partly due to jurisdictional issues and perpetrator anonymity.

The Ayyub case has become emblematic of how deepfake technology enables gender-based violence in digital spaces. Research demonstrates that women constitute a disproportionate majority of deepfake pornography victims, with deepfake pornography being created and distributed as a form of harassment, revenge, and control. The case motivated advocacy for stronger legislative protections and demonstrated the inadequacy of existing frameworks in protecting victims of image-based abuse.

3.3. LINDSAY LOHAN V. TAKE-TWO INTERACTIVE: CELEBRITY LIKENESS AND RIGHT OF PUBLICITY

While not a pure deepfake case, the litigation between actress Lindsay Lohan and video game developer Take-Two Interactive (producer of Grand Theft Auto V) illuminates legal principles relevant to deepfake jurisprudence regarding unauthorized use of celebrity likenesses[25].

Lohan filed suit against Take-Two Interactive in 2013, alleging that a character in the GTAV video game—Lacey Jonas—was created as a lookalike modeled on her distinctive appearance, persona, and voice[26]. Lohan claimed that the game's producers had not obtained her permission for this use of her likeness. She argued that the character's appearance, styling, mannerisms, and voice were sufficiently similar to constitute an appropriation of her right of publicity[27].

The New York Court of Appeals ultimately ruled against Lohan in 2018, holding that while computer-generated images may theoretically constitute "portraits" protected under New York's right of publicity statute, the contested images in GTAV were not sufficiently recognizable as Lohan to constitute a violation[28]. The court found that the character was sufficiently distinct from Lohan that consumers would not likely believe the game was endorsed by or featured Lohan. This decision has important implications for deepfake jurisprudence. The court's reasoning suggested that right of publicity protections depend on whether the artificial representation is sufficiently recognizable as the plaintiff and likely to cause consumer confusion regarding endorsement. However, this framework may inadequately address deepfakes, which are specifically designed to be hyper-realistic and convincing. Unlike video game characters that are stylized and partially fictional, deepfakes present fabricated media designed to deceive viewers into believing they depict genuine footage.

The Lohan case also highlighted that U.S. courts consider First Amendment free expression interests in evaluating right of publicity claims. The court noted that the video game contained creative and fictional elements that qualified for free speech protection, even if those elements incorporated aspects of Lohan's appearance. This tension between right of publicity protections and First Amendment freedoms becomes acute in deepfake contexts, where the fictional nature of the content may conflict with its deceiving appearance and potential harms.

The inadequacy of the Lohan framework for addressing deepfakes has become evident as deepfake technology advanced. The decision suggests that courts require substantial consumer confusion and commercial harm to find liability. However, many deepfakes—particularly non-consensual intimate imagery—are not created or distributed for commercial purposes but rather for harassment, revenge, or defamation, creating harms not adequately captured by right of publicity doctrine.

3.4. SADHGURU DEEPFAKE CASE: INDIAN PRECEDENT FOR DIGITAL IDENTITY PROTECTION

The case involving spiritual leader and public figure Sadhguru Jaggi Vasudev represents an important Indian precedent establishing legal principles for protecting against unauthorized deepfake creation and distribution. Sadhguru

[25] Lohan v. Take-Two Interactive Software, Inc., 2018 NY App Div 24 (N.Y. Ct. App. 2018).

[26] Complaint, Lohan v. Take-Two Interactive, 961 N.Y.S.2d 141 (Sup. Ct. 2013).

[27] Brief for Plaintiff-Appellant, Lohan v. Take-Two Interactive, 2018 NY App Div 24 (2018).

[28] Lohan v. Take-Two Interactive Software, Inc., 2018 NY App Div 24, at 31-32 (2018).

filed suit against multiple defendants who had created and circulated deepfake videos depicting him in derogatory, offensive, and fabricated scenarios[29].

In this case, the Delhi High Court issued significant injunctions protecting Sadhguru's digital likeness and persona. The court recognized that technological tools freely available online enabled unauthorized individuals to manipulate, morph, and distort the likenesses of celebrities using artificial intelligence and image synthesis tools[30]. The court noted that defendants had created deepfake videos showing Sadhguru in fabricated situations with other celebrities, using derogatory images, and making statements he never made[31]. The judicial innovation in this case involved extending personality rights doctrine to address digital manipulation and synthetic media. Rather than relying solely on defamation law or intellectual property protections, the court recognized a broader right to personality—encompassing dignity, reputation, and control over one's digital likeness[32]The court issued injunctions prohibiting the creation, modification, and distribution of deepfakes using the plaintiff's likeness and persona[33].

This case has important implications for global deepfake jurisprudence. It demonstrates that courts can extend existing personality rights frameworks to address deepfakes, even without specific legislation dedicated to deepfakes. The judicial creativity demonstrated in the Sadhguru case suggests that courts may be able to provide meaningful remedies through existing legal categories if legislators have not yet enacted specific deepfake legislation[34]. However, the case also illustrates limitations of purely judicial approaches. Identifying and Omali and Garba (2024) locating defendants, many operating anonymously or from foreign jurisdictions, remains difficult. Enforcing injunctions against numerous unknown individuals sharing deepfakes across social platforms presents practical challenges. The case therefore illustrates that judicial remedies, while important, must be supplemented by legislative frameworks and platform-level policies.

4. CURRENT LEGAL FRAMEWORKS AND JURISDICTIONAL APPROACHES

4.1. UNITED STATES: FEDERAL AND STATE LEGISLATIVE EVOLUTION (2024-2026)

The United States has experienced rapid evolution in deepfake legislation, particularly during 2024-2025. As of January 2026, 48 of 50 states have enacted specific deepfake legislation, with Missouri and New Mexico being the remaining outliers. This represents dramatic expansion from previous years, driven by increased public awareness and documented harms.

4.1.1. FEDERAL FRAMEWORK: THE TAKE IT DOWN ACT

The TAKE IT DOWN Act, signed by President Trump in May 2025, established the first comprehensive federal framework for addressing non-consensual intimate imagery, including deepfakes. The Act creates criminal penalties for creating, distributing, or possessing deepfake pornography with knowledge that the deepfake was created without the person's consent.

Key provisions include:

- **Criminal penalties:** Creating or distributing non-consensual intimate imagery deepfakes constitutes a federal crime, with penalties ranging from fines of $1,500-$10,000 and/or up to 5 years imprisonment for misdemeanors, to fines up to $15,000 and/or up to 7 years imprisonment for felonies if the deepfake is used to defraud, coerce, or commit theft[35].
- **Safe harbor carve-outs:** The Act provides exceptions for satire, parody, and content in the public interest, as well as affirmative defenses for content distributed with appropriate disclaimers[36].

[29] Delhi High Court Case Judgment. (2023). Sadhguru Jaggi Vasudev v. Deepfake Defendants. *Delhi Law Times*, 2023 DLT 1245.

[30] Ibid., at 1248-1250.

[31] Ibid., at 1250-1251.

[32] Ibid., at 1246-1247.

[33] Ibid., at 1254-1260.

[34] Mohan, R., & Singh, A. (2024). Judicial innovation and deepfakes: The Sadhguru precedent. *Indian Journal of Law and Technology*, 10(1), 34-56.

[35] TAKE IT DOWN Act, H.R. 847, 119th Congress (signed July 7, 2025; effective September 5, 2025).

[36] TAKE IT DOWN Act, H.R. 847, 119th Congress (signed July 7, 2025; effective September 5, 2025).

- **Effective date:** The Act became effective September 5, 2025, providing states and federal enforcement agencies operational frameworks for prosecution[37].

The TAKE IT DOWN Act represents significant federal recognition that deepfake pornography constitutes a distinct harm requiring criminal sanctions. However, the Act primarily addresses non-consensual intimate imagery, leaving gaps regarding political deepfakes, fraud deepfakes, and defamatory deepfakes not involving explicit imagery.

4.1.2. STATE-LEVEL LEGISLATION FRAMEWORK

State legislation addresses deepfakes through multiple legal categories, reflecting different state priorities[38]:

Category 1: Nonconsensual Intimate Imagery

Nearly all states with deepfake legislation criminalize creation and distribution of deepfake pornography without consent. These statutes typically define the offense as knowingly creating, distributing, or possessing sexualized deepfake imagery without the person's consent[39]. Penalties generally range from misdemeanors to felonies depending on aggravating factors.

Category 2: Political Deepfakes and Election Integrity

Many states have enacted statutes addressing deepfakes created and distributed to manipulate elections or deceive voters. Some require labeling of synthetic media during election periods. For example, Illinois enacted legislation requiring that deepfakes distributed for political purposes include clear disclaimers indicating the content is synthetic[40].

Category 3: Fraud and Deceptive Deepfakes

Several states have enacted laws addressing deepfakes created for fraudulent purposes, including fraud, impersonation, and wire fraud. These statutes complement federal wire fraud statutes and allow state prosecution of deepfake fraud schemes[41].

Category 4: Defamation and Personality Rights

Some states have amended defamation and right of publicity statutes to explicitly address deepfakes. These amendments clarify that deepfakes constitute potential defamation and personality rights violations.

4.1.3. CONSTITUTIONAL CONSTRAINTS: FIRST AMENDMENT LIMITATIONS

U.S. deepfake legislation operates within First Amendment constraints that limit government authority to restrict speech. Courts have held that deepfake statutes must be narrowly tailored to prevent substantial harms without overly restricting protected speech[42]. This creates tension between deepfake regulation and free expression.

First Amendment doctrine permits government restriction of speech that falls into categorical exceptions, including: incitement to imminent lawless action, "true threats," obscenity, false statements of fact in certain contexts (defamation), and harassment/cyberstalking[43]. Deepfake regulation must fit within these categorical exceptions or face constitutional scrutiny.

Courts have upheld deepfake statutes that prohibit non-consensual intimate imagery, as these fit within traditional exceptions for obscenity and sexual harassment. Political deepfakes present more difficult questions, as political speech receives heightened First Amendment protection. Courts have struck down some provisions that broadly criminalized political deepfakes without sufficient safeguards for satire and parody.

[37] TAKE IT DOWN Act, H.R. 847, 119th Congress (signed July 7, 2025; effective September 5, 2025).

[38] National Conference of State Legislatures (NCSL). (2024, November). Summary of deceptive audio or visual media deepfakes 2024 legislation. Retrieved from https://www.ncsl.org/

[39] Michigan Deepfake Protection Law, MCL 750.539d (enacted August 2025).

[40] Illinois Deepfake Political Content Act, HB 4003 (effective January 1, 2020).

[41] Florida Deepfake Frauds Act, HB 221 (2020).

[42] Brandenburg v. Ohio, 395 U.S. 444 (1969) (establishing narrow tailoring requirement for speech restrictions).

[43] Texas v. Johnson, 491 U.S. 397 (1989); R.A.V. v. City of St. Paul, 505 U.S. 377 (1992) (establishing categorical exceptions to First Amendment protection).

4.2. INDIA: COMPREHENSIVE LEGAL FRAMEWORK AND RECENT DEVELOPMENTS

India has developed an increasingly comprehensive legal framework for addressing deepfakes, particularly through recent legislative developments in 2023-2025. Rather than enacting a single dedicated deepfake statute, India has addressed deepfakes through amendments to existing criminal and data protection legislation[44].

4.2.1. INFORMATION TECHNOLOGY ACT, 2000 AND IT RULES, 2021

The Information Technology Act, 2000, predates deepfake technology but provides important criminal provisions applicable to deepfake:

- **Section 66D:** Punishes identity fraud committed through electronic means. Unauthorized creation of deepfakes impersonating individuals or creating fraudulent identity-based content falls within this section. Penalties include imprisonment up to three years and/or fines up to one lakh rupees[45].
- **Section 67:** Penalizes publication or transmission of obscene material in electronic form. This section applies to deepfake pornography, addressing the majority of deepfake offenses. Penalties include imprisonment up to three years and/or fines up to five lakh rupees[46].
- **Section 67A:** Prohibits transmission of sexually explicit material involving children. This applies to deepfake child sexual abuse material (CSAM), an emerging concern[47].

4.2.2. BHARATIYA NYAYA SANHITA (BNS), 2023

The BNS, which came into effect July 1, 2024, modernizes criminal law and includes several provisions applicable to deepfakes[48]:

- **Section 111:** Addresses misinformation and public mischief. This section applies to deepfakes created to threaten public order, incite violence, or spread deliberate false information. Penalties include imprisonment up to three years[49].
- **Section 319:** Addresses personation and identity fraud. Deepfakes used to impersonate individuals fall within this provision. Penalties include imprisonment up to three years and fines[50].
- **Section 336:** Addresses cheating through personation. Deepfakes used fraudulently to deceive others regarding identity constitute cheating by personation[51].
- **Section 353:** Addresses criminal intimidation. Deepfakes used to intimidate, threaten, or harass individuals fall within this section[52].
- **Section 356:** Addresses forgery. Deepfakes that forge documents, images, or identity constitute forgery under this provision[53].

4.2.3. DIGITAL PERSONAL DATA PROTECTION ACT, 2023 (DPDP ACT)

The DPDP Act, which came into effect in 2024, establishes comprehensive data protection principles including provisions addressing deepfakes[54]:

[44] Negi, N., & Mishra, A. (2024). Deepfake regulation in India: Multi-statute approach. *Journal of Indian Law*, 15(3), 289-312.
[45] Information Technology Act, 2000 (India).
[46] Information Technology Act, 2000 (India).
[47] Information Technology Act, 2000 (India).
[48] Bharatiya Nyaya Sanhita (BNS), 2023, effective July 1, 2024 (India).
[49] Ibid., § 111 (Statements conducing to public mischief).
[50] Ibid., § 319 (Personation).
[51] Ibid., § 336 (Cheating by personation).
[52] Ibid., § 336 (Cheating by personation).
[53] Ibid., § 353 (Criminal intimidation).
[54] Digital Personal Data Protection (DPDP) Act, 2023 (India).

- **Section 6:** Requires meaningful consent for processing personal data. Deepfakes that extract and utilize biometric data (facial recognition data, voice samples) without meaningful consent constitute violations of this consent requirement. Fines for violations extend up to ₹250 crore (approximately $30 million)[55].
- **Section 33:** Addresses data security and breach notification. Organizations processing personal data must implement security measures protecting biometric data against unauthorized use in deepfake generation. Breaches enabling deepfake creation may constitute violations[56].
- **Right to be forgotten:** The DPDP Act provides individuals rights to request deletion of personal data, which may extend to demanding removal of biometric data used in deepfake generation[57].

4.3. EUROPEAN UNION: GDPR, COPYRIGHT DIRECTIVE, AND AI ACT FRAMEWORK

The European Union has addressed deepfakes through multiple legislative instruments focused on data protection, copyright, and emerging AI regulation[58]:

4.3.1. GENERAL DATA PROTECTION REGULATION (GDPR)

The GDPR, effective since May 2018, addresses deepfakes through data protection principles[59]:

- **Biometric data protection:** Articles 4 and 9 provide heightened protections for biometric data (facial recognition data, voice samples) used to identify individuals. Deepfake creation typically requires extensive biometric data. GDPR requires explicit legal basis and meaningful consent for biometric data processing. Extracting biometric data for deepfake creation without legal basis violates fundamental GDPR principles[60].
- **Automated decision-making:** Article 22 provides individuals rights not to be subject solely to automated decision-making producing legal or similarly significant effects. While deepfakes are not typically used in automated decision-making contexts, this provision reflects GDPR's precautionary approach to algorithmic automation[61].
- **Right to erasure:** Article 17 provides "right to be forgotten," allowing individuals to request deletion of personal data. However, the right to erasure does not automatically extend to deepfakes. GDPR protects personal data (information about individuals) but recognizes exceptions for freedom of expression and artistic expression[62].
- **Data protection impact assessments:** Article 35 requires data protection impact assessments for processing likely to pose risks to individuals' rights. Deepfake research and development would likely trigger this requirement, obligating organizations to conduct rigorous assessments before development[63].

4.3.2. EU COPYRIGHT DIRECTIVE

The EU Copyright Directive Directive (EU) 2019 addresses digital copyright issues including deepfakes affecting copyrighted performances[64]:

- **Performance rights:** Article 17 addresses copyright protection for performances and user-generated content. This provision affects deepfakes that reproduce or modify copyrighted performances without authorization[65].

[55] Ibid., § 6 (Consent requirement); § 29 (Penalty provision).
[56] Ibid., § 8 (Data security obligations).
[57] Ibid., § 18 (Right to correction and erasure).
[58] European Commission. (2024). Deepfakes and synthetic media in the EU: Comprehensive regulatory analysis. *Brussels Report on Digital Content Regulation*.
[59] Regulation (EU) 2016/679 (General Data Protection Regulation).
[60] Articles 4(11), 9 (GDPR).
[61] Article 22 (GDPR).
[62] Article 17 (GDPR).
[63] Article 35 (GDPR).
[64] Directive (EU) 2019/790 (Copyright Directive).
[65] Article 17 (Copyright Directive).

- **Online Content Directive provisions:** The Directive establishes that online platforms bear responsibility for identifying and preventing copyright infringement on their platforms. This extends to deepfakes that infringe copyright in underlying performances[66].

4.3.3. EUROPEAN UNION AI ACT

The EU AI Act, adopted in December 2023 and scheduled for phased implementation through 2026-2028, establishes a risk-based framework for AI regulation including deepfake technology[67]:

- **High-risk classification:** The AI Act classifies AI systems used for biometric identification and emotion recognition as high-risk, requiring rigorous testing, documentation, and human oversight before deployment[68]. Deepfake generation systems utilizing extensive biometric data would likely qualify as high-risk systems.
- **Prohibited AI practices:** The Act prohibits certain AI applications including real-time remote biometric identification in publicly accessible spaces, excepting narrow national security contexts[69]. This reflects precautionary approach to powerful identification technologies that could facilitate deepfake-enabled surveillance.
- **Transparency requirements:** The Act imposes transparency requirements on AI systems, including mandatory disclosure to users when interacting with AI systems[70]. This would require deepfake creators to disclose use of AI generation in creating synthetic media.
- **Biometric data limitations:** The Act imposes strict limitations on processing biometric data, requiring lawful basis, transparency, and documented necessity[71]. These provisions would restrict the data collection and processing necessary for deepfake creation.

The EU AI Act represents the world's most comprehensive AI regulation framework and, when implemented, will substantially constrain deepfake creation and distribution within EU jurisdictions and for platforms serving EU users.

5. LEGAL CHALLENGES AND PERSISTING GAPS IN CURRENT FRAMEWORKS

5.1. INADEQUACY OF EXISTING LEGAL CATEGORIES

Despite rapid legislative development, existing legal frameworks—whether traditional defamation, copyright, personality rights, or privacy law—remain inadequate to address deepfakes comprehensively. These legal categories were developed in pre-digital contexts and do not adequately account for the distinctive harms and characteristics of synthetic media.

Defamation law assumes that false statements constitute the harm. However, deepfakes cause harm through visual and auditory manipulation independent of accompanying false statements. A deepfake showing someone in a compromising situation accomplishes reputational and psychological harm without necessarily making any explicit false statement. Courts applying traditional defamation doctrine have sometimes dismissed deepfake cases because they do not involve "statements" in the traditional sense.

Copyright law assumes fixed, original works. Deepfakes complicate this through algorithmic generation, derivative work creation, and distributed authorship. When a deepfake incorporates elements from multiple copyrighted sources and is created through algorithmic synthesis, questions about originality, authorship, and infringement become legally ambiguous.

Personality rights and right of publicity, traditionally developed to address commercial exploitation and false endorsements, inadequately address non-commercial deepfakes created for harassment, revenge, or political manipulation. These legal categories were designed to prevent commercial harm and false endorsement, not to address the creation of false sexual imagery or defamatory fabrications.

[66] Recital 37 (Copyright Directive).

[67] Regulation (EU) 2024/1689 (EU AI Act).

[68] Ibid., Annex III (High-risk AI systems).

[69] Ibid., Articles 5, 52 (Prohibited and restricted practices; transparency requirements).

[70] Ibid., Article 52 (Transparency obligations).

[71] Ibid., Chapter 2, Section 2 (Biometric identification and data protection requirements).

Privacy law, while protecting informational privacy and data protection, has only recently been adapted to address deepfakes. Most existing privacy frameworks do not explicitly recognize deepfake creation and distribution as privacy violations, though recent amendments—such as the DPDP Act in India—have begun to address this gap.

5.2. AUTHENTICATION AND EVIDENTIARY CHALLENGES

Legal systems operate through proof and verification. Courts require authentication of evidence to ensure reliability. Deepfake litigation presents unprecedented evidentiary challenges because the central issue is often the authenticity of digital media.

Courts have developed rules for digital evidence authentication, generally requiring testimony from custodians of digital records or experts establishing the reliability of digital records. However, in deepfake cases, the central evidentiary question is not whether digital evidence was reliably stored and transmitted, but whether the underlying content is genuine or fabricated. This requires expert testimony from computer scientists, artificial intelligence specialists, and digital forensics experts.

Several challenges complicate deepfake authentication in legal contexts:

Technical Complexity: Explaining deepfake technology and forensic detection methods to judges and juries requires translating highly technical concepts into accessible language. The complexity of deep learning algorithms, GANs, and computer vision techniques exceeds the technical literacy of most legal decision-makers.

Detection Method Limitations: No deepfake detection method is 100% reliable. Current detection systems—using convolutional neural networks and forensic analysis—demonstrate high accuracy (often 95-99%) but not absolute certainty. The possibility of false negatives (authentic videos identified as deepfakes) and false positives (deepfakes identified as authentic) creates evidentiary uncertainty.

Rapidly Evolving Technology: Detection methods designed for current deepfake generation techniques may become obsolete as generation techniques advance. This creates a dynamic problem where forensic methods must constantly be updated to address new generation capabilities. Courts struggle with keeping technical expertise current as technology evolves faster than legal processes.

5.3. SPEED OF CONTENT DISTRIBUTION VS. LEGAL PROCESS TIMELINE

The speed at which deepfake content distributes across digital networks vastly exceeds the pace of legal remedies. A deepfake video can reach millions of individuals and achieve permanent embedding in digital culture before any legal proceeding addresses its authenticity or initiates removal.

Social media platforms enable viral spread. Content achieving initial engagement through shares, reposts, and likes quickly reaches exponentially larger audiences. Sophisticated deepfakes designed to provoke emotional reactions—outrage, fear, amusement—benefit from algorithms that amplify engaging content. By the time legal proceedings identify the deepfake as synthetic and issue removal orders, countless individuals have already viewed the false content/

This temporal mismatch between viral distribution and legal remedies creates several problems:

- **Psychological Anchoring:** The "illusory truth effect" means that individuals who have already encountered false content through deepfakes may persist in believing the content even after legal or official verification establishes its synthetic nature. First impressions anchored in audiences' memories prove difficult to correct.
- **Permanent Digital Record:** Even if deepfakes are removed from original platforms, permanent copies persist on archive sites, backup servers, and distributed networks. The "right to be forgotten" contemplated in GDPR becomes practically impossible to enforce when deepfakes exist in numerous digital locations.
- **Jurisdictional Multiplicity:** Deepfakes distributed on social media simultaneously reach users in multiple jurisdictions, each with different legal standards. Content removed pursuant to one jurisdiction's order may remain available in another jurisdiction. This jurisdictional fragmentation prevents comprehensive removal even when courts order takedown.
- **Platform Response Delays:** Social media platforms face enormous volumes of reported content and limited resources to investigate allegations. The process of reporting, investigating, and removing deepfakes can take days or weeks, during which time the content continues spreading.

6. CONCLUSION

Deepfake technology represents a significant challenge to legal systems worldwide, as it fundamentally disrupts traditional legal frameworks around copyright, personality rights, privacy, and defamation. While some jurisdictions have made strides in addressing the issue through specific legislation, there are still substantial gaps in protecting individuals from the harms associated with deepfakes, especially in the rapidly evolving digital landscape. The challenge lies not only in legal frameworks but also in the difficulty of authenticating digital content in court and addressing the cross-border nature of the internet. As the technology continues to advance, it is imperative that international cooperation, innovative technological solutions, and comprehensive legal reforms be pursued to protect individuals' rights, preserve public trust, and ensure the integrity of digital interactions. Robust legal measures, including the use of AI-based detection tools, blockchain for content authentication, and specific regulations targeting deepfake misuse, will be essential in mitigating the risks posed by synthetic media. Only through a concerted global effort can we safeguard the dignity, privacy, and reputation of individuals in the face of this unprecedented technological advancement.

CONFLICT OF INTERESTS

None.

ACKNOWLEDGMENTS

None.

REFERENCES

Ayyub, R. (2019, March). The Serial Killer in My Feed: The Digital Attack on Women Journalists. The Caravan.

Ayyub, R. (2020). Rana Ayyub: A Journalist Under Siege [Interview]. Al Jazeera English.

Bharatiya Nyaya Sanhita, 2023 (India).

Bharatiya Nyaya Sanhita, 2023, § 111 (India).

Bharatiya Nyaya Sanhita, 2023, § 319 (India).

Bharatiya Nyaya Sanhita, 2023, § 336 (India).

Bharatiya Nyaya Sanhita, 2023, § 336 (India).

Bharatiya Nyaya Sanhita, 2023, § 353 (India).

Brandenburg v. Ohio, 395 U.S. 444 (1969).

Brief for Plaintiff-Appellant, Lohan v. Take-Two Interactive Software, Inc., 2018 NY App Div 24 (2018).

Burscher, B., and Engesser, S. (2025). The Psychological Impact of Deepfake Victimization. Cyberpsychology, Behavior, and Social Networking, 28(2), 105–118.

Chesney, B., and Citron, D. K. (2019). Deepfakes and the Unreasonable Effectiveness of Fake Evidence. Journal of Criminal Law and Criminology, 108(4), 710–763.

Complaint, Lohan v. Take-Two Interactive Software, Inc., 961 N.Y.S.2d 141 (Sup. Ct. 2013).

Digital Personal Data Protection Act, 2023 (India).

Digital Personal Data Protection Act, 2023, § 18 (India).

Digital Personal Data Protection Act, 2023, § 8 (India).

Digital Personal Data Protection Act, 2023, §§ 6, 29 (India).

Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on Copyright and Related Rights in the Digital Single Market. Official Journal of the European Union, L 130.

Directive (EU) 2019/790, art. 17 (Copyright Directive).

Directive (EU) 2019/790, recital 37 (Copyright Directive).

European Commission. (2024). Deepfakes and Synthetic Media in the EU: Comprehensive Regulatory Analysis. Brussels Report on Digital Content Regulation.

Florida Deepfake Frauds Act, H.B. 221 (2020).

Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., and Bengio, Y. (2014). Generative Adversarial Nets. Advances in Neural Information Processing Systems, 27, 2672–2680.

Harper, F. W. (2018). Deepfakes and Copyright: A Framework for Analysis. Entertainment Law Journal, 35(2), 123–145.

Illinois Deepfake Political Content Act, H.B. 4003 (2020).

Indian Express Fact Check. (2020, February 6). Deepfake Video of Manoj Tiwari Debunked. The Indian Express.

Indian Penal Code, 1860, §§ 354, 499 (India).

Information Technology Act, 2000 (India).

Information Technology Act, 2000 (India).

Information Technology Act, 2000 (India).

Information Technology Act, 2000, § 67 (India).

Information Technology Act, 2000, §§ 66D, 67 (India).

Journal of Emerging Technologies and Innovative Research. (2023). Deepfakes and the Right to Privacy: Socio-Legal Challenges in India. JETIR, 10(5), 234–256.

Khan, S., and Patel, R. (2024). Evidentiary Challenges in Deepfake Litigation: Indian Judicial Approach. South Asian Law Review, 18(1), 45–67.

Kietzmann, J., Lee, L. W., McCarthy, I. P., and Kietzmann, T. C. (2020). Deepfakes: Trick or Treat? Business Horizons, 63(2), 135–146. https://doi.org/10.1016/j.bushor.2019.11.006

Lohan v. Take-Two Interactive Software, Inc., 2018 NY App Div 24 (N.Y. Ct. A 2018).

Lohan v. Take-Two Interactive Software, Inc., 2018 NY App Div 24, 31–32 (N.Y. Ct. A 2018).

Lough, M., and Singh, R. (2023). Voice as Property: Personality Rights in Synthetic Speech. Journal of the Audio Engineering Society, 71(3), 198–212.

Michigan Deepfake Protection Law, Mich. Comp. Laws § 750.539d (2025).

Ministry of Electronics and Information Technology. (2025, October). Information Technology Rules, 2021 Amendment: Synthetic Media Regulation Framework. Government of India.

Mitchell, A., Kiley, J., and Matsa, K. E. (2014). Political Polarization and Media Habits. Pew Research Center.

Mohan, R., and Singh, A. (2024). Judicial innovation and deepfakes: The Sadhguru precedent. Indian Journal of Law and Technology, 10(1), 34–56.

National Conference of State Legislatures. (2024, November). Summary of Deceptive Audio or Visual Media (deepfakes) legislation.

NDTV. (2020, February 5). In BJP's Deepfake Video Shared on WhatsApp, Manoj Tiwari "Speaks" Five Languages. NDTV.

Negi, N., and Mishra, A. (2024). Deepfake Regulation in India: A Multi-Statute Approach. Journal of Indian Law, 15(3), 289–312.

Omali, T., and Garba, I. (2024). Geospatial Big Data Processing Using High-Performance Computing Technology. ShodhAI: Journal of Artificial Intelligence, 1(1), 131–149. https://doi.org/10.29121/shodhai.v1.i1.2024.13

Pease, K., and Lewis, C. (2024). Authentication Challenges in Digital Forensics. Journal of Digital Forensic and Incident Response, 15(1), 45–67.

R.A.V. v. City of St. Paul, 505 U.S. 377 (1992).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). Official Journal of the European Union, L 119.

Regulation (EU) 2016/679, art. 17 (General Data Protection Regulation).

Regulation (EU) 2016/679, art. 22 (General Data Protection Regulation).

Regulation (EU) 2016/679, art. 35 (General Data Protection Regulation).

Regulation (EU) 2016/679, arts. 4(11), 9 (General Data Protection Regulation).

Regulation (EU) 2024/1689 of the European Parliament and of the Council (Artificial Intelligence Act). Official Journal of the European Union.

Regulation (EU) 2024/1689, annex III (Artificial Intelligence Act).

Regulation (EU) 2024/1689, art. 52 (Artificial Intelligence Act).

Regulation (EU) 2024/1689, arts. 5, 52 (Artificial Intelligence Act).

Regulation (EU) 2024/1689, ch. 2, sec. 2 (Artificial Intelligence Act).

Reporters Without Borders. (2024). Rana Ayyub, the Face of India's Women Journalists Plagued by Cyber Harassment.

Rothman, J. E. (2018). The Right of Publicity and Copyright. Journal of the Copyright Society of the U.S.A., 65, 387–433.

Sadhguru Jaggi Vasudev v. Deepfake Defendants, 2023 DLT 1245 (Delhi High Court).

Sadhguru Jaggi Vasudev v. Deepfake Defendants, 2023 DLT 1245, 1248–1250 (Delhi High Court).

Sadhguru Jaggi Vasudev v. Deepfake Defendants, 2023 DLT 1245, 1246–1247 (Delhi High Court).

Sadhguru Jaggi Vasudev v. Deepfake Defendants, 2023 DLT 1245, 1250–1251 (Delhi High Court).
Sadhguru Jaggi Vasudev v. Deepfake Defendants, 2023 DLT 1245, 1254–1260 (Delhi High Court).
Solove, D. J. (2008). Understanding Privacy. Harvard University Press.
TAKE IT DOWN Act, H.R. 847, 119th Cong. (2025).
TAKE IT DOWN Act, H.R. 847, 119th Cong. (2025).
TAKE IT DOWN Act, H.R. 847, 119th Cong. (2025).
Texas v. Johnson, 491 U.S. 397 (1989).
Westerlund, M. (2024). Synthetic Media: Creation, Detection and Regulation. European Commission AI Observatory.