ILE INTELLECTUAL PROPERTY AND CORPORATE LAW REVIEW
VOLUME 4 AND ISSUE 1 OF 2025
APIS – 3920 – 0008 | ISSN – 2583–6153

Published by
Institute of Legal Education
https://iledu.in

DEEPFAKES AND INTELLECTUAL PROPERTY RIGHTS: OWNERSHIP, AUTHORSHIP, AND LEGAL AMBIGUITIES

AUTHOR – SHIVANI GUPTA, RESEARCH SCHOLAR AT IFTM UNIVERSITY, MORADABAD, U.P,

BEST CITATION - SHIVANI GUPTA, DEEPFAKES AND INTELLECTUAL PROPERTY RIGHTS: OWNERSHIP, AUTHORSHIP, AND LEGAL AMBIGUITIES, *ILE INTELLECTUAL PROPERTY AND CORPORATE LAW REVIEW,* 4 (1) OF 2025, PG. 46-56, APIS – 3920 – 0008 | ISSN – 2583–6153.

ABSTRACT

Deepfake technology, which leverages artificial intelligence to manipulate or fabricate video and audio content, poses significant legal and ethical questions. Among the most complex is the question of intellectual property rights (IPR): *Who owns the fake?* This paper delves into the evolving legal landscape in India surrounding deepfakes, analyzing them through the prism of copyright law, moral rights, personality rights, and image rights. It further identifies the statutory and regulatory gaps in the current Indian framework and evaluates how well existing intellectual property laws can respond to the challenges posed by such AI-generated content. Drawing upon Indian statutes, judicial precedents, and comparative international approaches, the paper proposes a framework that balances innovation with legal and ethical safeguards. As digital content creation and manipulation through artificial intelligence continues to expand, the paper underscores the urgent need for a comprehensive regulatory response within the Indian context.

Keywords: Deepfakes, Intellectual Property Rights (IPR), Copyright Law, Moral and Personality Rights, Artificial Intelligence and Law, Regulatory Framework in India.

1. Introduction

Deepfakes represent a novel technological frontier in synthetic media. Powered by deep learning algorithms, particularly generative adversarial networks (GANs), deepfakes can produce hyper-realistic images, videos, and audio clips that mimic real individuals,often with alarming accuracy. GANs work by pitting two neural networks against each other: a generator, which creates fake content, and a discriminator, which evaluates its authenticity. Over successive iterations, the system learns to create convincingly realistic media that can be nearly indistinguishable from authentic footage.

This technology has evolved rapidly. Originally developed for harmless applications such as face-swapping in entertainment and special effects, deep fakes are now being used for a wide range of purposes from satirical parodies and voice synthesis to digital resurrection of deceased actors and personalized advertising. However, with such capabilities come significant ethical and legal challenges. Deep Fakes are increasingly being misused for non-consensual pornography, political misinformation, celebrity impersonation, financial fraud, and identity theft, raising concerns about privacy, consent, authenticity, and reputation.

In the Indian context, where digital media consumption is surging and AI adoption is accelerating, these concerns become especially urgent. The country's existing legal framework, rooted in traditional notions of authorship and originality, has yet to adequately address the complexities introduced by synthetic media.

Central to the legal inquiry is the question: *Who owns the rights over deepfake content?* Is it the

ILE INTELLECTUAL PROPERTY AND CORPORATE LAW REVIEW
VOLUME 4 AND ISSUE 1 OF 2025
APIS – 3920 – 0008 | ISSN – 2583–6153
Published by
Institute of Legal Education
https://iledu.in

creator of the deepfake, the subject whose likeness is used, or the developer of the AI tool? Indian copyright law, moral rights, and personality rights provide partial guidance, but they often fall short when applied to AI-generated and manipulated works. This paper seeks to analyze the legal ambiguities surrounding deepfakes under Indian intellectual property law and explore the broader implications for ownership, liability, and regulatory reform.

This research analyzes:

a. The applicability of Indian copyright law to deep fakes.

b. The conflict between deepfake creators and individuals whose likenesses are used.

c. Regulatory gaps and potential legal reform

2. Legal Framework in India

India lacks a dedicated legal framework governing AI-generated content or synthetic media like deepfakes. Existing laws under the Copyright Act, the Information Technology Act, and tort law offer fragmented remedies but fail to provide a comprehensive approach. This necessitates an examination of current statutes and their limitations.

3. Copyright Law and Deepfakes

3.1. Copyright Act, 1957

The primary statute governing copyright in India is the **Copyright Act, 1957**[1].

a. Authorship and Ownership

Section 2(d) defines an author as the individual responsible for creating a work. However, in the context of cinematographic films and computer-generated content, the term "author" typically refers to the producer or the person who initiates or facilitates the creation of the work.

b. Originality Requirement

The landmark case Eastern Book Company v. D.B. Modak[2] established that for a work to qualify as "original" under Indian copyright law, it must exhibit a minimum degree of creativity and not merely involve labor or skill. The Court adopted a "modicum of creativity" standard, moving away from the older "sweat of the brow" doctrine. This has significant implications for deepfake content, which is predominantly generated by artificial intelligence with minimal direct human involvement beyond the initial training of the model. Since the AI autonomously creates the final output, and the human input is often indirect or functional, deep fakes may fail to satisfy the threshold of originality as defined in Modak, thereby rendering them ineligible for copyright protection under current Indian law.

c. Fixation Requirement

While Indian law does not explicitly require fixation, courts have assumed fixation to be essential. Deepfakes, once stored digitally, satisfy this requirement.

d. AI as Author?

Indian law currently does not acknowledge non-human entities as authors. This raises a complex question when a work is created using AI, who holds authorship? Is it the AI system itself, the programmer who developed the AI, or the individual who provided the input data that guided its creation?

3.2. Authorship of AI-Generated Content

a. No Clear Precedent: Unlike the U.S. (where the Copyright Office denies AI copyright), India has no explicit stance.

b. Possible Solutions:

- Recognize AI developers as authors (as in the UK).
- Treat deepfakes as derivative works requiring consent.

3.3. Moral Rights under Indian Copyright Laws

Under the Copyright Act, 1957, authors enjoy not only economic rights over their work but also moral rights, which are recognized under

ILE INTELLECTUAL PROPERTY AND CORPORATE LAW REVIEW
VOLUME 4 AND ISSUE 1 OF 2025
APIS – 3920 – 0008 | ISSN – 2583–6153
Published by
Institute of Legal Education
https://iledu.in

Section 57. These rights, often described by the French term *droit moral*, stem from the philosophical notion that a creative work is an expression of the author's personality and therefore merits protection beyond monetary considerations. Indian law codifies this through statutory moral rights, which continue even after the transfer or sale of the economic rights.

a. "Scope of Moral Rights under Section 57

Section 57 of the Copyright Act, 1957 grants authors two fundamental moral rights:

- Right of Paternity: The right to claim authorship of a work.

Right of Integrity: The right to prevent any distortion, mutilation, or other modification of the work that would be prejudicial to the author's honor or reputation.

These rights are independent of the author's ownership status" and remain enforceable even if the economic rights in the work have been assigned or licensed to another party .

b. Application to Deepfakes

The proliferation of deepfake technology, which allows hyper-realistic digital manipulation of audio-visual media, introduces complex challenges for moral rights. In cases where a deep fake alters the visual appearance, voice, or expression of a public figure in a derogatory or misleading manner, it is arguable that this could constitute a violation of moral rights.

Although Section 57 traditionally applies to distortions of copyrighted works, if the manipulated content is based on a prior performance, film, or audiovisual work in which a public figure has contributed, then alteration via deep fakes may compromise the integrity of that work.

Examples include:

- A deep fake video placing a famous actor in a fabricated obscene or controversial scene, thereby distorting their original performance.
- Altering a politician's speech to falsely depict them endorsing contentious opinions, impacting their reputation and public perception.

Such scenarios can be viewed as undermining the author's integrity and artistic contribution, potentially triggering moral rights protections.

c. Judicial Interpretation and Potential Extension

"The Delhi High Court's ruling in Amarnath Sehgal v. Union of India[4] remains the cornerstone of moral rights jurisprudence in India. In this case, the court emphasized the artist's enduring connection to their creation and upheld their right to object to mutilation of their work by the government, even after it had been transferred."

Although Indian courts have not yet adjudicated deepfakes within the scope of Section 57, the principles elucidated in *Amarnath Sehgal* could form the basis for future extensions. Courts may interpret moral rights to cover cases where:

- A deepfake uses content derived from a copyrighted performance or audiovisual work.
- The manipulation causes reputational harm or artistic misrepresentation.
- The affected individual is recognized as an author or contributor to the original protected work.

d. Limitations and Challenges

Despite the potential for extending moral rights to cover deep fakes, several limitations persist:

a. **Work vs. Likeness**: Moral rights attach to works, not personalities. When a deepfake uses a person's likeness or voice without drawing on a prior copyrighted work, invoking Section 57 becomes legally difficult.

b. **Free Speech Concerns**: Expanding moral rights to curb deepfakes may unintentionally restrict legitimate forms of expression such as parody, satire, or political commentary. Courts will have to balance moral rights against Article 19(1)(a) of the Indian

ILE INTELLECTUAL PROPERTY AND CORPORATE LAW REVIEW
VOLUME 4 AND ISSUE 1 OF 2025
APIS – 3920 – 0008 | ISSN – 2583–6153
Published by
Institute of Legal Education
https://iledu.in

Constitution[5], which guarantees freedom of speech and expression.

c. **Technological Ambiguity**: Identifying authorship, originality, and the source of AI-generated deep fakes adds another layer of complexity to moral rights enforcement.

4. Personality Rights and Deep fakes

4.1. Right to Publicity vs. Right to Privacy

Indian courts recognize personality rights under Article 21 (Right to Life) and tort law:

- R. Rajagopal v. State of Tamil Nadu[6]: Recognized an individual's right to control the use of their name, image, and likeness.
- Titan Industries v. Ramkumar Jewellers[7]: Recognized unauthorized use of a celebrity's persona for commercial gain as infringement of personality rights.

Deep fakes that use a person's face or voice without consent, especially in defamatory, commercial, or misleading ways, can thus amount to a violation of image and personality rights.

Indian jurisprudence has increasingly acknowledged personality rights which include the right to control the commercial use of one's name, image, likeness, and other personal attributes under the broader umbrella of Article 21 of the Constitution (Right to Life and Personal Liberty) and through tort law. In *R. Rajagopal v. State of Tamil Nadu* (1994), the Supreme Court expressly recognized an individual's right to privacy and autonomy, affirming that individuals possess the right to control how their identity is portrayed or published. This ruling laid the foundation for personality rights in India by asserting that unauthorized publication of a person's image or life details, especially without consent, amounts to a violation of the right to privacy.

Further reinforcing this position, the Delhi High Court in *Titan Industries Ltd. v. Ramkumar Jewellers* (2012) held that the unauthorized commercial exploitation of a celebrity's persona including their name, image, and likeness amounted to a clear infringement of their publicity rights. The Court emphasized that such rights are distinct and protect the individual's identity from misuse for trade or advertising purposes without permission.

In the context of deepfakes, which can convincingly replicate a person's facial expressions, voice, and mannerisms using artificial intelligence, these legal protections become critically relevant. When deepfakes are created or disseminated without the subject's consent— particularly for defamatory, misleading, pornographic, or commercial purposes they can constitute a direct violation of that person's image rights, right to privacy, and publicity rights. Such use not only damages personal reputation but may also lead to psychological distress, loss of professional opportunities, or unauthorized commercial exploitation of a person's identity. Despite this, India still lacks a comprehensive legislative framework that explicitly protects personality rights in digital contexts, making the enforcement of such rights against deepfake misuse a growing legal challenge.

4.2. Case Study: Anil Kapoor vs. AI-Generated Deep fakes

In 2023, actor Anil Kapoor approached the Delhi High Court seeking protection from unauthorized AI-generated deepfake videos that depicted him endorsing products and saying inappropriate things. The court granted an interim injunction and recognized his right to control his likeness, setting a precedent for personality rights enforcement in the context of AI.

5. Regulatory Framework and Gaps

Sections 66E and 66D of the Information Technology Act[8] address certain cybercrimes involving privacy and impersonation. Section 66E penalizes the violation of privacy by

criminalizing the capturing, publishing, or transmission of private images without the consent of the individual concerned. This provision is aimed at safeguarding an individual's right to privacy in the digital realm. On the other hand, Section 66D deals with impersonation using communication devices, specifically targeting fraudulent activities carried out through digital means, such as identity theft or deception for personal gain. However, a significant limitation of the IT Act lies in its inability to keep pace with emerging technological threats. The Act does not explicitly account for modern challenges such as AI-generated impersonations or the creation and dissemination of synthetic media, commonly referred to as "deep fakes." This has resulted in interpretational gaps and enforcement challenges, as existing legal provisions may not adequately cover these technologically advanced forms of deception and privacy invasion.

5.1. The Digital India Act (DIA)

The draft legislation is anticipated to introduce AI-specific provisions aimed at addressing the growing concerns around synthetic and deepfake content. One of the key measures expected is mandatory watermarking, which would require all AI-generated or synthetic media including deepfakes to carry identifiable digital watermarks. This would enhance traceability and help differentiate between authentic and manipulated content, thereby promoting transparency and Accountability in digital communications. Another significant provision under consideration is platform liability. Under this framework, digital platforms that host user-generated content could be held accountable for the dissemination of malicious deep fakes. These platforms would be obligated to implement prompt takedown mechanisms and ensure that harmful or deceptive synthetic content is removed swiftly. Together, these proposed measures reflect a policy shift towards curbing the misuse of AI technologies while balancing the responsibility between content creators and hosting intermediaries.

6. Criminal Implications and Data Protection

6.1. Information Technology Act, 2000

The Information Technology Act, 2000 establishes a legal framework to combat various cyber offenses, including privacy breaches and the circulation of obscene content. Specifically, Section 66E penalizes violations of privacy by prohibiting the unauthorized capturing, sharing, or transmission of images of an individual's private parts without their consent, particularly when such actions infringe on the person's privacy. Meanwhile, Section 67 deals with the publication or transmission of obscene material in electronic form, prescribing penalties for such conduct on digital platforms.

In the context of deep fakes, particularly those used for revenge porn, fake news, or sexually exploitative purposes, these provisions become especially relevant. Deepfakes that depict individuals in explicit or compromising scenarios without their consent may constitute a breach of privacy under Section 66E and also amount to the electronic dissemination of obscene content under Section 67, thereby attracting legal consequences under both sections.

6.2. Right to Privacy

"The right to privacy has been firmly established as a fundamental right under Article 21 of the Indian Constitution following the landmark judgment in Justice K.S. Puttaswamy (Retd.) v. Union of India[9]. This case established privacy as intrinsic to the right to life and personal liberty." The creation and circulation of deep fakes, particularly those that manipulate a person's likeness without their knowledge or consent, directly infringe this right. By distorting an individual's identity and misrepresenting their actions or speech, deep fakes pose a serious threat to personal dignity, autonomy, and informational self-determination, all of which are essential components of the right to privacy.

ILE INTELLECTUAL PROPERTY AND CORPORATE LAW REVIEW
VOLUME 4 AND ISSUE 1 OF 2025
APIS – 3920 – 0008 | ISSN – 2583–6153
Published by
Institute of Legal Education
https://iledu.in

7. Comparative Jurisprudence

7.1. United States

"In the United States, the legal response to deep fakes is still developing, with legislation varying from state to state. One notable protection is the Right of Pub*licity*, recognized in several states, which safeguards individuals against the unauthorized commercial use of their name, image, voice, or other distinctive aspects of their identity. This right becomes Particularly relevant in deep fake scenarios where a person's likeness is used without permission, especially for profit-driven or deceptive purposes. In 2019, the Deepfake Accountability Act[10] was introduced in an effort to establish clearer standards around the labeling and traceability of AI-generated content; however, the bill has not yet been enacted into law. Additionally, under U.S. copyright law, the U.S. Copyright Office maintains that works generated solely by artificial intelligence without meaningful human authorship are not eligible for copyright protection. This creates a significant legal gap in addressing ownership and accountability for AI-generated content."

7.2. European Union

The European Union provides one of the most comprehensive and robust data protection frameworks in the world through the General Data Protection Regulation (GDPR)[11]. The GDPR ensures strong safeguards for personal data, including identifiable elements such as voice and image. Under this framework, the creation and dissemination of deepfakes using an individual's likeness or biometric data without explicit, informed consent constitutes a violation of the data subject's rights. This positions the EU as a region with strict legal accountability mechanisms for misuse of AI and synthetic media. The GDPR's emphasis on lawful processing, purpose limitation, and data minimization provides a comprehensive basis to challenge and penalize unauthorized deep fake usage.

7.3. United Kingdom

In the United Kingdom, copyright protection is governed by the Copyright, Designs and Patents Act, 1988[12]. According to Section 9(3) of the Act, a work must have a human author in order to qualify for copyright protection, thereby excluding purely AI-generated content from legal ownership claims unless a human creator can be identified. This principle highlights the challenges in attributing authorship and enforcing intellectual property rights in the context of AI. The UK's stance underscores an important lesson for India: there is a pressing need to establish clear definitions of authorship, ownership, and the protection of personal likeness in AI-generated content. As AI technologies evolve rapidly, jurisdictions like India must develop forward-looking legal frameworks to address the complex intersection of privacy, identity, and artificial creativity.

7.4. Canada

In Canada, the legal framework surrounding deepfakes intersects primarily with copyright and privacy laws. Under the Copyright Act, RSC 1985, c C-42[13]copyright protection is granted only to works created by a human author. "The Canadian Intellectual Property Office (CIPO) has maintained that copyright must stem from original expression and human creativity, thereby excluding purely AI-generated content from protection unless there is substantial human" contribution involved. This limitation creates ambiguity when addressing ownership of deepfake content created autonomously by AI systems.

From a privacy perspective, while Canada does not have a specific federal statute addressing deep fakes, provincial privacy and personality rights laws particularly in provinces like British Columbia, Manitoba, Newfoundland and Labrador, and Saskatchewan can offer recourse in cases involving the unauthorized use of a person's likeness, name, or voice. Such protections are rooted in common law torts, such as "misappropriation of personality," which

ILE INTELLECTUAL PROPERTY AND CORPORATE LAW REVIEW
VOLUME 4 AND ISSUE 1 OF 2025
APIS – 3920 – 0008 | ISSN – 2583–6153
Published by
Institute of Legal Education
https://iledu.in

have been recognized by Canadian courts, as seen in Krouse v. Chrysler Canada Ltd. (1973)[14], where the Ontario Court of Appeal upheld a claim for unauthorized commercial use of an individual's image.

However, the absence of a unified legal response to deepfakes at the federal level reveals a significant legislative gap. Canadian lawmakers have acknowledged the growing influence of generative AI and are in the process of consulting stakeholders on potential reforms. "The Artificial Intelligence and Data Act (AIDA)[15], introduced as part of Bill C-27 (Digital Charter Implementation Act, 2022)[16]", proposes a regulatory framework for "high-impact" AI systems, but it does not directly address copyright or ownership concerns related to AI-generated media. As such, Canada remains in a transitional phase, with an urgent need for legal clarity in areas of authorship, ownership, and personality rights in the era of deepfakes.

7.5. Australia

Australia's legal landscape concerning deepfakes and intellectual property rights is currently fragmented, lacking a comprehensive statutory response specific to AI-generated content. "Under the Copyright Act 1968 (Cth), copyright subsists in original works made by human authors." The Australian Copyright Office and the courts have reiterated that originality must derive from human intellectual effort, thus excluding entirely AI-generated content from copyright protection. This was highlighted in the Telstra Corporation Limited v Phone Directories Company Pty Ltd (2010)[17]case, where the Federal Court emphasized that a "human author" must be identified for copyright to subsist.

In terms of privacy and personality rights, Australia does not recognize a standalone right of publicity. However, individuals may seek remedies under the common law tort of "misuse of private information", or through Australian Consumer Law (ACL) provisions addressing misleading and deceptive conduct, particularly if deep fakes are used for commercial deception. Additionally, Australia's Office of the eSafety Commissioner has begun tackling synthetic media harms, particularly in the context of non-consensual deepfake pornography, under the Online Safety Act 2021[18].

Despite these fragmented protections, Australia's 2023 consultation paper on copyright and emerging technologies indicates a governmental recognition of the pressing need to reconsider legal definitions of authorship, ownership, and liability in the age of AI.[19]

7.6. China

"China has adopted a proactive and multifaceted approach to regulating deepfakes and synthetic media, combining elements of intellectual property law and cybersecurity regulations.Under the Copyright Law of the People's Republic of China (amended in 2020)[20]"maintains that copyright protection requires human authorship, the government has gone further to address synthetic media via administrative regulations. In January 2023, the Cyberspace Administration of China (CAC) implemented the "Provisions on the Administration of Deep Synthesis Internet Information Services"[21], which mandate that deep fake content be clearly labeled and traceable, and that service providers ensure no infringement of personal rights occurs.

These rules, coupled with China's Civil Code (2021)[22], which recognizes "the right to one's name, image, and voice, allow individuals" to bring claims against unauthorized deepfake usage under personality rights law. Additionally, deepfake production that infringes upon state interests or individual reputation may lead to administrative and even criminal sanctions under China's Cybersecurity Law and Criminal Law.[23]

While China lacks clarity on the ownership of purely AI-generated works, the state's aggressive regulation of deepfake technology

highlights a control-oriented yet forward-thinking approach to AI governance.

7.7. Japan

In Japan, the Copyright Act (Act No. 48 of 1970) [24]emphasizes that copyright protection applies only to works created through "creative expression by humans", effectively excluding autonomous AI-generated content from ownership under current law. The Agency for Cultural Affairs clarified in 2019 that non-human generated works do not qualify for copyright, although AI-assisted works involving human input may still qualify depending on the extent of that input.[25]

Japan's Civil Code and Act on the "Protection of Personal Information (APPI)" [26]provide some protection against the unauthorized use of an individual's likeness or biometric data in deepfakes. While Japan does not yet have specific legislation addressing deepfakes, courts have increasingly accepted claims based on moral rights, defamation, and privacy violations, particularly where a deepfake misleads or harms reputation.

In 2023, "Japan's Ministry of Economy, Trade and Industry (METI)" launched discussions on AI and copyright, recognizing the legal vacuum around generative technologies and suggesting reforms that may address authorship and liability issues in the future.[27]

8. Ownership of Deepfakes: Legal Analysis

Scenario	Possible Owner	Legal Justification
AI-generated deep fake with no human input	No one	Lacks originality and human authorship; does not meet criteria under Indian copyright law
Deepfake using dataset and human-curated model	User/Trainer	Considered closest to authorship "under Section 2(d) of the Copyright Act, 1957."
Deep fake of a celebrity used for commercial purposes	Celebrity	Protected under image rights and the right of publicity; unauthorized use amounts to misappropriation
Parodic or artistic deepfake	Contextual (Fair Use)	May fall under fair dealing exceptions if used for satire,
		commentary, or art, and no reputational harm occurs

9. Policy Recommendations

9.1. Legislative Reforms

To effectively address the challenges posed by deepfakes and AI-generated content, legislative reform is essential. One key recommendation is to amend the *Copyright Act, 1957* to recognize AI-generated works, provided there is identifiable human attribution or creative input. This would help clarify ownership and protect intellectual property in cases involving human-guided AI outputs. Additionally, there is a pressing need for statutory recognition of *personality rights*, including image, voice, and publicity rights, under intellectual property or standalone legal frameworks. This would ensure legal protection for individuals,especially public figures— whose likeness is used without consent, particularly for commercial or

deceptive purposes.

9.2. Regulatory Measures

From a regulatory standpoint, platforms that host user-generated content must be held accountable for the dissemination of harmful or malicious deepfakes. Regulations should mandate swift takedown procedures upon receiving credible complaints or reports of such content. Furthermore, there should be a legal requirement for *consent and watermarking* of synthetic media. This would involve embedding digital watermarks in AI-generated content for traceability and ensuring that personal data, such as images or voices, is used only with explicit consent.

9.3. Institutional and Societal Initiatives

Beyond legal and regulatory frameworks, institutional and societal interventions are crucial. Public awareness campaigns should be launched to educate users about the ethical creation, use, and detection of deepfakes. These initiatives should aim to foster digital literacy and resilience against misinformation. On the judicial front, *fast-track redressal mechanisms* should be instituted for cases where deepfakes result in reputational or financial harm. Swift judicial remedies will act as a deterrent and provide timely relief to affected individuals, ensuring that the legal system keeps pace with the technological threat landscape.

10. Conclusion

Deep fakes present a complex and evolving challenge to traditional legal frameworks, particularly in areas concerning intellectual property, privacy, and data protection. While current Indian laws such as the Copyright Act and the Information Technology Act provide limited tools for redress, they fall short when it comes to clearly defining the ownership, authorship, and liability of AI-generated content,especially in cases where human involvement is minimal or non-existent. Despite these gaps, certain individual rights, such as the fundamental right to privacy under Article 21 and the emerging recognition of publicity and image rights, continue to offer some degree of legal protection against unauthorized and harmful deepfake use.

As India advances rapidly in digital innovation and AI integration, the legal ecosystem must keep pace. Comprehensive reform is urgently needed to address the nuanced intersection of artificial intelligence, creative ownership, personal autonomy, and legal accountability. This reform must include amendments to intellectual property laws, regulatory frameworks for platform responsibility, and robust privacy safeguards. Ultimately, the most critical question facing lawmakers, technologists, and society at large is: **"Who owns the fake?"** Answering this will be pivotal to ensuring both innovation and individual rights are preserved in the age of synthetic media.

Bibliography

Indian Statutes and Government Frameworks

- Copyright Act, 1957 (India).
- Information Technology Act, 2000 (India).
- Constitution of India, Articles 19(1)(a) and 21.
- Digital India Act (Draft, 2023), Ministry of Electronics and Information Technology (MeitY), Government of India.

Indian Case Law

- *Eastern Book Company v. D.B. Modak*, (2008) 1 SCC 1.
- *Amarnath Sehgal v. Union of India*, 2005 (30) PTC 253 (Del).
- *R. Rajagopal v. State of Tamil Nadu*, (1994) 6 SCC 632.
- *Titan Industries Ltd. v. Ramkumar Jewellers*, 2012 SCC OnLine Del 2387.
- *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
- *Anil Kapoor v. Various Platforms & Persons*, Delhi High Court, 2023.

International Legislation and Policy Documents

- Deepfake Accountability Act, H.R.3230, 116th Congress (United States, 2019).
- U.S. Copyright Office, Policy Statement on Registration of AI-Generated Works, 2023.
- General Data Protection Regulation (GDPR), Regulation (EU) 2016/679.
- Copyright, Designs and Patents Act 1988 (United Kingdom).
- Artificial Intelligence and Data Act (AIDA), Bill C-27, Digital Charter Implementation Act, 2022 (Canada).
- Copyright Act 1968 (Cth), Australia.
- Provisions on the Administration of Deep Synthesis Internet Information Services (China, 2023).
- Civil Code of the People's Republic of China (2021).
- Copyright Act (Act No. 48 of 1970), Japan.
- Act on the Protection of Personal Information (APPI), Japan.

International Case Law

- *Krouse v. Chrysler Canada Ltd.*, [1973] O.J. No. 1962 (Ontario Court of Appeal, Canada).
- *Telstra Corporation Ltd. v. Phone Directories Company Pty Ltd.*, [2010] FCAFC 149 (Federal Court of Australia).

Academic and Scholarly Sources

- Gervais, Daniel J. "The Machine As Author." *Iowa Law Review*, vol. 105, no. 5, 2020, pp. 2053–2086.
- Saval, Melissa. "Deepfakes and the Law: A Call for Legislative Action." *Harvard Journal of Law & Technology*, vol. 34, no. 2, 2021.
- Bhandari, Neha. "AI and the Indian Legal Framework: Bridging the Governance Gap." *NLIU Law Review*, vol. 10, no. 2, 2022.
- Jain, Anuradha. "Personality Rights and Deep Fakes: India's Legal Vacuum." *Indian Journal of Law and Technology*, vol. 19, 2023.

Reports and News Articles

- Bar and Bench. "Delhi HC Grants Interim Relief to Anil Kapoor Against AI-Generated Deepfakes." October 2023. https://www.barandbench.com
- The Hindu. "India Plans AI Regulations Under New Digital India Act." April 2024. https://www.thehindu.com
- Economic Times. "AI and Copyright: What the Draft DIA Means for Digital Creators." February 2024. https://economictimes.indiatimes.com

ENDNOTES

1The Copyright Act, 1957 (India).

2Eastern Book Company v D B Modak (2008) 1 SCC 1 (SC).

4 Amarnath Sehgal v Union of India (2005) 30 PTC 253 (Del).

5 The Constitution of India, 1950.

6 R. Rajagopal v. State of Tamil Nadu,(1994) 6 SCC 632.

7 Titan Industries Ltd v Ramkumar Jewellers (2012)SCC OnLine Del 2381

8 The Information Technology Act 2000 (India)

9 Justice K S Puttaswamy (Retd) v Union of India (2017) 10 SCC 1 (SC)

10Deepfake Accountability Act 2019, HR 3230, 116th Cong (USA, not enacted)

11 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [2016] OJ L119/1

12 Copyright, Designs and Patents Act 1988, s 9(3) (UK),

13 Copyright Act, RSC 1985, c C-42.

14 Krouse v Chrysler Canada Ltd (1973) 1 OR (2d) 225 (Ont CA)

15 Canadian Intellectual Property Office, Canadian Intellectual Property Office Guidelines (2025) https://www.ic.gc.ca/eic/site/cipointernet-internetopic.nsf/eng/home accessed 15 April 2025.

16 Bill C-27: Digital Charter Implementation Act, 2022 (Part III: Artificial Intelligence and Data Act)

17 Telstra Corporation Limited v Phone Directories Company Pty Ltd [2010] FCA 44 (Fed Ct, Aust)

18 Online Safety Act 2021 (Cth) (Austl).

19 Australian Government, 'Copyright and Emerging Technologies: Consultation Paper' (2023).

20 Copyright Law of the People's Republic of China (Amended 2020), Standing Committee of the National People's Congress.

21 Cyberspace Administration of China (CAC), Provisions on the Administration of Deep Synthesis Internet Information Services (effective 10 January 2023).

22 Civil Code of the People's Republic of China (promulgated May 28, 2020, effective Jan 1, 2021).

23 Cybersecurity Law (China, 2016); Criminal Law of the People's Republic of China (rev. 2020).

24 Copyright Act 1970 (Act No. 48 of 1970) (Japan).

25 Agency for Cultural Affairs (Japan), 'Copyright in the Era of AI: Discussion Document' (2019).

26 Act on the Protection of Personal Information (APPI) 2003 (Japan); Civil Code (Japan).

27 Ministry of Economy, Trade and Industry (Japan), 'Report on AI and Copyright Reform Proposals' (2023)