Research article

Maharaja Surajmal Institute Law Journal
Year 2025, Volume-2, Issue-1 (January-June)

Online ISSN: 3048-9105

Digital Identity Rights: A Comparative Analysis of Denmark's and India's Approaches to Deepfakes

Manindra Singh Hanspal[1]* and Devendra Singh Tomar[2]

[1]Assistant Professor, School of Law, Presidency University, Bengaluru. ORCID iD: 0009-0002-5973-807X
[2]Practicing Advocate, High Court of Madhya Pradesh

ARTICLE INFO

Keywords: Deepfakes, Digital Identity Rights, Copyright Law, Biometric Likeness Protection, Comparative Legal Analysis

Doi: 10.48165/msilj.2025.2.1.3

ABSTRACT

The proliferation of generative artificial intelligence has enabled sophisticated deepfake technology, posing unprecedented challenges to digital identity protection and personal autonomy. This comparative legal analysis examines Denmark's 2025 copyright reforms, introducing biometric likeness protection, against India's fragmented legal framework for addressing deepfake-related digital impersonation. Through doctrinal legal research and comparative methodology, this study analyzes Denmark's innovative Sections 73a and 65a of the Copyright Act, which extend intellectual property rights to protect facial features, voice, and physical characteristics from unauthorized digital imitation. The research reveals significant gaps in India's current legal landscape, where privacy rights, defamation laws, and information technology provisions provide only piecemeal protection against AI-generated identity theft. Denmark's consent-based model, offering post-mortem protection for 50 years and establishing precise takedown mechanisms, presents a robust framework that balances individual rights with technological innovation. The findings demonstrate that India's adoption of similar copyright-based personality rights could substantially enhance digital identity protection while maintaining compatibility with global regulatory standards. The study offers policy-relevant insights for jurisdictions grappling with AI, intellectual property, and human dignity.

INTRODUCTION

1.1 Background

The digital revolution has ushered in an era of unprecedented technological advancement, with generative artificial intelligence emerging as one of the most transformative yet concerning developments of the 21st century.[1] At the forefront of this technological evolution lies deepfake technology, which utilizes sophisticated machine learning algorithms and neural networks to create hyper-realistic but fabricated audio, video, and image content. The sophistication of these AI-generated manipulations has

*Corresponding author.
email id: mhanspal21@gmail.com

reached alarming levels, with modern deepfake systems capable of producing content that is virtually indistinguishable from authentic material to the untrained eye.[2] The exponential growth in deepfake technology has been accompanied by a corresponding surge in malicious applications, ranging from nonconsensual intimate imagery to political disinformation campaigns.[3] Recent incidents, such as the fabricated video of actor Rashmika Mandanna that circulated across social media platforms in November 2023, have highlighted the immediate and tangible threats posed by this technology to individual dignity and privacy.[4] These developments have catalyzed urgent discussions among legal scholars, policymakers, and technology experts about the adequacy of existing legal frameworks to address the multifaceted challenges posed by AI-generated content. The traditional legal paradigms governing privacy, defamation, and intellectual property were conceived in an analog era and have proven inadequate to address the unique challenges presented by deepfake technology.[5]

1.2. Significance of the Study

The significance of this research lies in its examination of two contrasting approaches to deepfake regulation, offering insights into the evolution of digital rights protection in an increasingly AI-dominated landscape. Denmark's pioneering legislative approach, which grants individuals copyright protection over their biometric features, including face, voice, and physical characteristics, represents a landmark shift in how legal systems conceptualize and protect digital identity. This innovative framework has been recognized as providing "a potential blueprint for Europe and beyond" in addressing the complex intersection of artificial intelligence, intellectual property rights, and personal autonomy. The study's focus on India provides a critical counterpoint, examining how one of the world's largest digital economies grapples with deepfake challenges through its existing legal infrastructure. This comparative analysis contributes to the emerging global discourse on AI governance by examining how different legal traditions and regulatory philosophies approach the fundamental question of digital identity protection. The study's significance extends beyond academic inquiry, offering practical insights for policymakers, legal practitioners, and technology companies navigating the complex landscape of AI regulation and digital rights enforcement.

1.3. Research Objectives

This research pursues three primary objectives that collectively aim to advance understanding of effective legal responses to deepfake technology:

- To conduct a comprehensive analysis of Denmark's innovative copyright-based approach to digital identity protection, examining the legal mechanisms, enforcement procedures, and theoretical foundations underlying the country's landmark legislative reforms.
- To evaluate the adequacy and effectiveness of India's current legal framework in addressing deepfake-related digital impersonation, with particular attention to recent judicial precedents and regulatory initiatives.
- To develop evidence-based policy recommendations for enhancing India's legal framework through the adoption of elements from Denmark's model while ensuring compatibility with India's constitutional framework, existing legal structures, and socio-economic realities.

1.4. Research Questions

This study is guided by three interconnected research questions that frame the comparative analysis and policy development components of the research:

- How does Denmark's copyright reform address deepfake-related digital identity issues, and what legal innovations does this approach introduce to the broader framework of intellectual property protection?
- How does India currently address issues related to deepfakes, and what specific gaps in its legal framework limit adequate protection of digital identity rights?
- What elements of Denmark's model can be effectively adapted to India's legal and cultural context, and what modifications would be necessary to ensure successful implementation?

[1] A. S. Alalaq, "The history of the artificial intelligence revolution and the nature of generative AI work"2 DS Journal of Artificial Intelligence and Robotics1–24 (2024).
[2] P. Carpenter, FAIK: A Practical Guide to Living in a World of Deepfakes, Disinformation, and AI-Generated Deceptions (John Wiley & Sons, 2024).
[3] S. I. U. Mansoor, "Legal implications of deepfake technology: In the context of manipulation, privacy, and identity theft" 4 Central University of Kashmir Law Review 65–92 (2024).
[4] "Govt asks social media firms to identify, remove misinformation, deepfakes within 36 hrs," The Economic Times (8 Nov. 2023) https://economictimes.indiatimes.com/news/india/govt-asks-social-media-firms-to-identify-remove-misinformation-deepfakes-within-36-hrs/articleshow/105046833.cms?-from=mdr
[5] N. Afshari and A. Mohammadi, "The Legal Implications of Deepfake Technology: Privacy, Defamation, and the Challenge of Regulating Synthetic Media" 2 Legal Studies in Digital Age 13–23 (2023).

THE RISE OF DEEPFAKES AND THE NEED FOR DIGITAL IDENTITY PROTECTION

2.1. Definition and Technology Behind Deepfakes

Deepfake is a portmanteau of deep learning and fake, created with the help of deep neural networks (DNN), which are a part of machine learning (ML).[6] Deepfakes are technically based on deep neural networks, which reduce the difference between natural and artificial images.[7] Recent developments in deepfake technology have generated highly manipulated images, audio recordings, and video files that rely on artificial intelligence to create convincing forgeries of other people performing actions or making claims they never actually did.[8] The sophistication of these deepfake systems has reached such levels that they can look so realistic that spotting them as fake can be very challenging for humans, fundamentally altering the landscape of digital content authenticity.[9] The impact of deepfake technology extends across multiple sectors, with particularly significant implications for politics, entertainment, and media. Deepfake methods cause harm by enabling the creation of videos that fundamentally misrepresent reality (Springer, 2024), posing unprecedented challenges for content verification and trust systems in digital communication.[10]

2.2 Risks Posed by Deepfakes

- **Personal Harms:** Deepfake technology enables malicious actors to develop convincing fabricated content that can cause severe reputational damage, emotional distress, and privacy violations.[11] These personal harms are particularly concerning because they can be perpetrated without the victim's knowledge and may be difficult to detect or counter once the content begins circulating. Women and marginalized communities face disproportionate targeting through deepfake technology, with women, both in the public eye and as private citizens, being particularly vulnerable to malicious deepfake creation.[12] The gendered nature of deepfake abuse reflects broader patterns of online harassment while introducing new dimensions of harm enabled by AI technology.[13]
- **Public Harms:**Beyond individual victimization, deepfakes pose significant threats to public institutions and democratic processes.[14] Artificial intelligence deepfakes are a threat to elections, with the technology being deployed to influence political outcomes by spreading false information about candidates and public figures.[15] Deepfake technology has facilitated advanced disinformation campaigns that can even disrupt democratic voting and act as propaganda, creating divisions and doubt.[16] The political consequences of such interference at the national security level are broader than mere interference in the electoral process because state enemies or politically interested persons may also publish fake videos of elected officials or other people in power making inflammatory statements or committing other forms of misconduct.[17] These kinds of activities may undermine public faith, negatively influence the national discourse, and undermine the principles of democratic rule.

2.3. The Need for Legal Frameworks

Inadequacy of Existing Laws

Traditional legal frameworks developed for analog-era challenges prove fundamentally inadequate when con-

[6] A. Heidari, N. Jafari Navimipour, H. Dag and M. Unal, "Deepfake detection using deep learning methods: A systematic and comprehensive review" 14 Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery e1520 (2024).

[7] M. Masood, M. Nawaz, K. M. Malik, A. Javed, A. Irtaza and H. Malik, "Deepfakes generation and detection: State-of-the-art, open challenges, countermeasures, and way forward" 53 Applied Intelligence 3974–4026 (2023).

[8] A. Mohammed, "Deep Fake Detection and Mitigation: Securing Against AI-Generated Manipulation" 4 Journal of Computational Innovation (2024).

[9] A. S. George and A. H. George, "Deepfakes: the evolution of hyper realistic media manipulation" 1 Partners Universal Innovative Research Publication 58–74 (2023).

[10] M. A. Farouk and B. M. Fahmi, "Deepfakes and media integrity: Navigating the new reality of synthetic content" 3 Journal of Media and Interdisciplinary Studies (2024).

[11] G. Yadav, M. Z. Sadique, S. Kumar, R. Sharma, M. Sharma, R. Sharma and T. Rattan, "Psychological Trauma and Legal Challenges of Deep fake Technology" 37 Sciences of Conservation and Archaeology 143–150 (2025).

[12] L. Lazard, R. Capdevila, E. L. Turley, K. Gilfoyle and N. Stavropoulou, "Deepfake Technology and Gender-Based Violence: A Scoping Review" Trauma, Violence & Abuse 1 (2025).

[13] M. S. Akter and P. Ahmed, "The emergence of AI-generated deepfakes as a new tool for gender-based violence against women: A brief narrative review of evidence and the implications of the techno-feminist perspective" 13 feminists@law (2025).

[14] M. Pawelec, "Deepfakes and democracy (theory): How synthetic audio-visual media for disinformation and hate speech threaten core democratic functions" 1 Digital Society 19 (2022).

fronted with the unique characteristics of deepfake technology.[18] Conventional privacy laws, defamation statutes, and intellectual property protections were conceived within paradigms that assumed clear distinctions between authentic and fabricated content, making them ill-equipped to address the sophisticated nature of AI-generated synthetic media.[19] Current legal remedies often require proof of intent, damage, or specific forms of harm that may be difficult to establish in deepfake cases.[20] The speed at which synthetic content can be created and disseminated often outpaces legal systems' ability to respond effectively, creating a temporal mismatch between harm and remedy that can render traditional legal protections ineffective.

The Copyright Law Innovation

The recognition of these limitations has prompted innovative legal approaches that reconceptualize the relationship between technology, identity, and legal protection.[21] The lack of regulation exposes the country to election rigging and the dismantling of politics, highlighting the urgent need for comprehensive legal frameworks specifically designed to address AI-generated content.[22] Denmark's pioneering approach represents a fundamental shift in legal thinking, extending copyright protection to encompass biometric characteristics and digital identity.[23] The copyright-based approach offers several advantages over traditional privacy or defamation frameworks, including more precise enforcement mechanisms, established international treaty structures, and well-developed jurisprudential foundations.[24] By treating digital identity as intellectual property, this approach opens new possibilities for proactive protection rather than reactive remediation.

Denmark's Copyright Law Reform: A Path Forward For Digital Identity Protection

3.1. Overview of Denmark's Legal Reforms (2025)

Denmark has become an international leader in addressing the deepfake dilemma by enacting innovative legislation that effectively transforms the relationship between copyright law and personal identity, treating each person as the legal owner of their physical appearance, face, body, and voice.[25] The proposed amendments to the Copyright Act that the Danish Parliament presented in July 2025 are likely to be finalized this fall and introduced by the end of 2025. A first of its kind in Europe, the legislation will treat biometric characteristics as copyrightable content, setting a precedent that may influence legislative practices in the entire European Union and beyond.[26] The reform presents two essential clauses to the Copyright Act of Denmark, united in a collective consideration of the individual and professional issues associated with deepfake technology.[27] Section 73a of the proposed Danish Copyright Act amendment bill covers realistic digitally generated imitations of personal characteristics and states that "Realistic digitally generated imitations of the personal, physical characteristics of natural persons shall not be offered to the public without agreement.[28] Simultaneously, the legislation includes enhanced protections for performing artists through amendments that safeguard their professional

[15] M. B. E. Islam, M. Haseeb, H. Batool, N. Ahtasham and Z. Muhammad, "AI threats to politics, elections, and democracy: a blockchain-based deepfake authenticity verification framework" 2 Blockchains 458–481 (2024).

Ibid.

[17] R. Chesney and D. Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security" 107 California Law Review 1753–1819 (2019), available at https://www.californialawreview.org/print/deep-fakes-a-looming-challenge-for-privacy-democracy-and-national-security

[18] F. A. Ahmed, "Cybersecurity, data, and intellectual property: Where do the boundaries lie?" 6 Journal of Media Horizons 19–31 (2025).

[19] S. Pate, "Platform Liability for Platform Manipulation" 125 Columbia Law Review 873–924 (2025).

[20] J. Langa, "Deepfakes, real consequences: Crafting legislation to combat threats posed by deepfakes" 101 Boston University Law Review 761 (2021).

[21] J. Babikian, "Navigating legal frontiers: exploring emerging issues in cyber law" 17 Revista Española de DocumentaciónCientífica 95–109 (2023).

[22] E. Rumick, "What Happens When Robots Lie? Combatting the Harmful Threats of AI-Generated Disinformation While Harnessing Its Potential" 25 Journal of Law & Society 146 (2025).

[23] M. Bryant, "Denmark to tackle deepfakes by giving people copyright to their own features," The Guardian, 27 June 2025, https://www.theguardian.com/technology/2025/jun/27/deepfakes-denmark-copyright-law-artificial-intelligence

[24] D. J. Gervais, Re-structuring Copyright: A Comprehensive Path to International Copyright Reform (Edward Elgar Publishing, 2017).

[25] Andrea Willige, "Deepfake legislation: Denmark moves to protect digital identity," World Economic Forum (30 July 2025), https://www.weforum.org/stories/2025/07/deepfake-legislation-denmark-digital-id

[26] "Explained: How Denmark plans to use copyright law to protect against deepfakes," The Indian Express (2025), https://indianexpress.com/article/explained/explained-law/explained-how-denmark-plans-to-use-copyright-law-to-protect-against-deepfakes-10126883/

[27] "Denmark copyright crusade against deepfakes," Vajirao Institute UPSC Current Affairs, https://www.vajiraoinstitute.com/upsc-ias-current-affairs/denmark-copyright-crusade-against-deepfakes.aspx

[28] "The Danish Copyright Act: New ban on deepfakes and protection of artistic performances," Bech-Bruun (2025),https://www.bechbruun.com/en/news/news/the-danish-copyright-act-new-ban-on-deepfakes-and-protection-of-artistic-performances

[29] "When fitness meets national security: The growing threat of lifestyle-app data breaches," MyPrivacy.blog (2025), https://www.myprivacy.blog/when-fitness-meets-national-security-the-growing-threat-of-lifestyle-app-data-breaches/

identities and artistic expressions from unauthorized digital replication. Danish Culture Minister Jakob Engel-Schmidt has articulated the philosophical foundation underlying this legislative innovation, stating that "Human beings can be run through the digital copy machine and be misused for all sorts of purposes, and I am not willing to accept that".[29] This statement reflects a broader commitment to preserving human dignity and autonomy amid increasing technological sophistication and potential misuse.

3.2. Core Protection and Enforcement

- **Imitation Protection Framework:**The cornerstone of Denmark's approach is comprehensive protection against unauthorized digital imitation. This framework establishes a precise legal mechanism for individuals to assert control over their digital representation, providing both preventive and remedial measures against unauthorized use.[30] The legislation adopts a broad definition of protected characteristics, encompassing facial features, voice patterns, and other distinctive physical attributes that could be subject to digital replication. The suggested act considers a deepfake a realistic digital image of an individual, covering both appearance and voice to address every facet of the issue. With the updated copyright system, the Danish population would have the right to ask digital platforms to take down nonconsensual deepfaked messages.[31]
- **Performance Protection for Artists:**Recognizing the particular vulnerability of performers and artists to deepfake exploitation, the Danish legislation includes specific protections for artistic performances. The bill protects performing artists from the sharing of realistic, digitally generated imitations of their artistic performances without their consent.[32] Section 65 of the proposed amendment to the Danish Copyright Act determines that realistic digitally generated imitations of the artistic performance of a performing artist or a performer should not be made available to the general public without the permission of the performing artist or the performer.[33]
- **Enforcement Mechanisms and Legal Remedies:**The Danish approach emphasizes practical enforceability through precise procedural mechanisms and remedy structures. While the amendments do not directly provide for compensation or imprisonment, they allow individuals and performing artists to seek a legal remedy by demanding that illegal digital imitations be removed from social media and other platforms, with parties able to recover damages.[34] The act protects unlicensed recreation of artistic performances that are non-authoritarian in nature, and victims may claim remedies.

3.3 Legal, Ethical, and Social Implications of the Danish Law

- **Balancing Individual Rights and Collective Interests:**Denmark's approach represents a careful calibration of competing interests in the digital age, seeking to protect individual autonomy while preserving space for legitimate uses of AI technology.[35] The copyright-based approach offers distinct advantages in this balancing act, as intellectual property law has historically provided frameworks for balancing creator rights with public interest through concepts such as fair use, parody exceptions, and time-limited protection periods.[36] The Danish model's emphasis on consent provides individuals with a mechanism to maintain control over their digital representation while allowing authorized uses that serve legitimate purposes.[37]

[30] "Copywrong: Denmark's deepfake strategy for protecting identity," Thip.law (2025), https://thip.law/insights/copywrong-denmarks-deepfake-strategy-for-protecting-identity/
[31] Bryant, supra note 23.
[32] "Fighting deepfakes through the Danish Copyright Act," Kromann Reumert (2025), https://kromannreumert.com/en/news/fighting-deepfakes-through-the-danish-copyright-act
[33] "The Dutch / Danish proposals — legislation on deepfakes," DPO-India.com (PDF), https://dpo-india.com/Resources/Fines_and_Penalties_by_DPAs_on_Privacy_Violations/Netherlands-DPA/The-Dutch-Danish-proposals-legislation-deepfakes.pdf
[34] "The Danish Copyright Act: New ban on deepfakes and protection of artistic performances," Mondaq (2025), https://www.mondaq.com/copyright/1683228/the-danish-copyright-act-new-ban-on-deepfakes-and-protection-of-artistic-performances
[35] R. F. Jørgensen, "Data and rights in the digital welfare state: the case of Denmark" 26 Information, Communication & Society 123–138 (2023).
[36] W. M. Landes and R. A. Posner, The Economic Structure of Intellectual Property Law (Harvard University Press, 2003).
[37] E. Bietti, "Consent as a free pass: Platform power and the limits of the informational turn" 40 Pace Law Review 310 (2019).
[38] Bryant, supra note 23.
[39] Willige, supra note 25.
[40] "Denmark copyright crusade against deepfakes," supra note 27.
[41] F. Romero Moreno, "Generative AI and deepfakes: a human rights approach to tackling harmful content" 38 International Review of Law, Computers & Technology 297–326 (2024).
[42] H. Lauritsen, D. Hestbjerg, L. Pinborg and C. Pisinger, "A Policy Analysis of the Danish National AI Strategy: Ethical and Governance Implications for AI Ecosystems" 12 International Journal of Artificial Intelligence 24–36 (2025).
[43] J. J. Vinolia, "Unmasking Digital Deception: Legal Accountability of Social Media Platforms for Deep Fake Content" 5 Jus Corpus Law Journal 157 (2024).
[44] M. Dhir and S. Verma, AI for Good: India and Beyond—Detailed Analysis of AI & Laws, Policies, Ethical Frameworks and Judgements (Notion Press, 2024).

- **Setting Global Precedents:**As of July 2025, Denmark has introduced the likeness copyright proposal in Parliament, and the bill has gained traction in public. [38] The Danish approach could serve as a model for other jurisdictions grappling with similar challenges, particularly within the European Union. The landmark law is designed to strengthen protections against the creation and dissemination of deepfakes, establishing principles that could inform similar initiatives across different legal systems.[39]

3.4. Challenges and Criticisms

- **Enforcement in a Global Digital Environment:**Despite its innovative approach, Danish legislation faces significant challenges in enforcement. The proposed amendment may affect enterprises' use of the technology, but it may also offer protection against misuse.[40] The global nature of AI development and deployment means that Danish citizens may encounter deepfake content created in jurisdictions without equivalent protections, limiting the reach of domestic legal remedies. This challenge underscores the need for international cooperation and harmonized approaches to AI governance.[41]
- **Balancing Innovation and Protection:**Critics of the Danish approach raise concerns about potential negative impacts on technological innovation and creative expression. The challenge lies in establishing enforcement mechanisms that effectively deter harmful uses while preserving space for beneficial applications of AI technology. The long-term success of the Danish model will likely depend on its ability to evolve with technological developments while maintaining effectiveness in protecting individual rights.[42]

India's Current Legal Framework For Addressing Deepfakes

4.1. Overview of India's Legal Landscape

India's approach to deepfake regulation exemplifies the challenges faced by many jurisdictions attempting to address AI-generated content through existing legal structures developed for pre-digital contexts.[43] Currently, deepfakes are not addressed by any Indian legislation, forcing courts and legal practitioners to rely on a fragmented array of constitutional provisions, criminal law statutes, and information technology regulations to address harms caused by deepfakes.[44] The constitutional foundation for deepfake protection in India rests primarily on Article 21 of the Constitution, which guarantees the right to life and personal liberty. The unauthorized creation of deepfakes violates the right to privacy guaranteed under Article 21 of the Constitution, establishing a fundamental rights basis for protection that courts have increasingly recognized in personality rights cases.[45]

India's primary legislative instrument for addressing digital crimes, the Information Technology Act of 2000 (IT Act), contains several relevant provisions, though none were specifically designed to address AI-generated content. [46] The IT Act in Sections 67, 67A, and 67B are against the publication and transmission of obscene or sexually explicit content, which is a crime. Section 66E of the IT Act imposes a penalty for the infringement of the privacy of an individual by posting or sending an image of the private area of such an individual without his or her permission, with a maximum term of 3 years of imprisonment and a fine of INR 2 lakh.[47] While this provision offers some protection against nonconsensual intimate imagery,

[45] M. Srikant, "Bharatiya laws against deepfake cybercrime: Opportunities and challenges," VIF India (28 April 2025), https://www.vifindia.org/article/2025/april/28/Bharatiya-Laws-Against-Deepfake-Cybercrime-Opportunities-and-Challenges
[46] P. K. Chauhan, "AI and Cybercrime: A Comparative Analysis of Indian, EU, and US Regulatory Models" 6 NyaayShastra Law Review (2025).
[47] D. R. Bharati, "Violation of Privacy in Cyberspace (Section 66E of the IT Act, 2000)" (2025), available at https://ssrn.com/abstract=5390209
[48] N. Thapliyal, "Delhi High Court: Anil Kapoor's voice & image misuse — personality rights," LiveLaw (2024), https://www.livelaw.in/top-stories/delhi-high-court-anil-kapoor-voice-image-misuse-personality-rights-238217
[49] Pooja C., A. Reeta S. and C. Shruti, "Generative AI, Copyright and Personality Rights: A Comparative Legal Perspective" Legal Issues in the Digital Age 3, 23–51 (2025).
[50] JurAce Legal LLP, "Personality Rights in India & Beyond: Intellectual Property Dimensions," LinkedIn (22 Sept. 2025), https://www.linkedin.com/pulse/personality-rights-india-beyond-intellectual-property-dyihc/
[51] K. Simha, "Digital Age: Navigating Legal Landscape vis-à-vis Addressing Deepfakes and Manipulated Media" 12 Center for Development Economic 22–29 (2025).
[52] Dhir and Verma, supra note at 44.
[53] Mansoor, supra note at 3.
[54] Supra at 47.
[55] D. Kumar, "Deepfakes, Free Speech, and the Right to Truth: A Comparative Legal Study on Regulating Synthetic Media in the USA, UK, and India" 6 Advanced International Journal for Research (AIJFR) (July–Aug. 2025).
[56] Ib id.
[57] C. Busch, F. Deravi, D. Frings, E. Kindt, R. Lessmann, A. Nouak, et al., "Facilitating free travel in the Schengen area—A position paper by the European Association for Biometrics" 12 IET Biometrics 112–128 (2023).
[58] G. Hristov, "Genuine Harms Behind Artificial Content: How EU Regulation Can Combat Malicious Use of Deep Fake Technology" (2025), Available at SSRN 5634715.
[59] Y. Reinfeld and A. Gaon, The European Union and Digital Law: Normative Power in a Globalized Technological Landscape (Taylor & Francis, 2025).

its scope remains limited to specific types of privacy violations. It does not comprehensively address the broader spectrum of deepfake harms.

4.2. Existing Remedies and Judicial Precedents

The Anil Kapoor Case: A Landmark in Personality Rights

The Delhi High Court's decision in Anil Kapoor vs. Simply Life India and Others represents a watershed moment in Indian jurisprudence regarding personality rights and digital identity protection. The Delhi High Court issued an interim order safeguarding the personality rights of Bollywood actor Anil Kapoor and barred several other entities involved in abusing his image, name, voice, or other properties, establishing essential precedents for how Indian courts can address deepfake-related personality violations.[48] Significantly, in response to Kapoor's suit seeking protection of his personality rights, the Delhi HC restrained the use of AI tools to manipulate his images, directly addressing the deepfake challenge within the broader framework of personality rights protection.[49] The judgment's implications extend beyond celebrity protection to establish broader principles for digital identity rights. AI and deepfake technologies are developing at an alarming rate, and personality rights infringement is cutting across industries outside of the entertainment industry.

The Amitabh Bachchan Precedent:

Building on earlier precedents, the Anil Kapoor case follows the trail blazed by similar personality rights litigation involving other prominent figures. Anil Kapoor, actor-producer, had sued to protect his publicity/personality rights thereafter after Amitabh Bachchan (LinkedIn, 2023), demonstrating the growing judicial recognition of the need to protect individual identity in the digital age.[50] These cases collectively establish that Indian courts are prepared to extend personality rights protection to encompass threats to digital identity, even in the absence of specific legislative frameworks addressing deepfakes. The judicial approach has been pragmatic, utilizing existing legal doctrines while acknowledging the novel challenges posed by AI-generated content.

4.3. Limitations of Current Laws in Protecting Digital Identity

Gaps in Legislative Coverage

India's legal system has several gaps that hinder effective protection against deepfakes, despite judicial creativity in cases involving personality rights. However, there is no direct legislation against deepfakes in India.[51] Within the existing legislation, Sections 67 and 67A of the Information Technology Act 2000 punish the publication of sexually explicit content electronically, underscoring the ad hoc quality of existing protection.[52] The existing legal provisions address only specific categories of deepfake harm, primarily focusing on obscene or sexually explicit content while leaving other forms of malicious use unaddressed. Under the existing laws, the punishment for deepfake-related offences in India can be imposed only through expansive judicial interpretation, placing the burden on courts to interpret existing statutes creatively rather than providing clear legislative guidance.[53]

Enforcement Challenges:

The fragmented nature of India's approach creates significant enforcement challenges. In accordance with Sections 67 and 67A of the IT Act, 2000, the publication or transmission of obscene material (including deepfake pornography) online is subject to a maximum sentence of five years of imprisonment and a fine of 10 lakh.[54] However, these penalties apply only to specific categories of content and may not address other harmful uses of deepfake technology. Section 66D of the IT Act addresses individuals who use communication devices or computer resources maliciously to deceive or impersonate (Khurana & Khurana, 2024), providing some coverage for impersonation-based harms but lacking the specificity needed to address the sophisticated nature of AI-generated identity theft.[55] The practical application of these provisions requires extensive judicial interpretation, as evidenced by the fact that a fine of up to ₹2 lakh or up to three years in jail are the possible penalties for this kind of offence. In contrast, those who use computer resources or communication devices maliciously to impersonate someone or cheat are subject to punishment under Section 66D of the IT Act.[56]

A COMPARATIVE ANALYSIS: DENMARK VS. INDIA'S APPROACH TO DEEPFAKES

5.1. Key Differences in Legal Frameworks

- **Scope of Protection:**The fundamental distinction between Denmark's and India's approaches lies in the comprehensiveness and specificity of their

respective legal frameworks. Denmark's innovative legislation provides holistic protection for biometric characteristics through copyright law, establishing clear ownership rights over facial features, voice patterns, and physical attributes.[57] This approach creates a unified legal framework that explicitly addresses deepfakes, rather than attempting to fit AI-generated content into existing legal categories designed for different purposes. In contrast, India's fragmented approach relies on a patchwork of constitutional rights, criminal law provisions, and information technology regulations. While judicial precedents like the Anil Kapoor case demonstrate creative legal interpretation, the absence of specific deepfake legislation creates inconsistencies in protection and enforcement. The reactive nature of India's approach requires victims to pursue relief through multiple legal avenues, each with different standards of proof, remedies, and procedural requirements.

- **Consent-Based Framework:** Denmark's emphasis on consent represents a fundamental philosophical difference in how it approaches digital identity protection. The Danish model requires explicit consent for the creation and dissemination of deepfake content, establishing clear presumptions about individual control over digital representation.[58] This proactive approach empowers individuals to make informed decisions about their digital identity while providing clear legal boundaries for content creators and platforms. India's current framework lacks a comprehensive consent-based model for deepfake content. While privacy laws incorporate consent principles, and personality rights cases recognize the importance of authorization, there is no unified consent framework specifically addressing AI-generated content.
- **Global Applicability and Enforcement:** Denmark's integration into the European Union's legal frameworks provides advantages for cross-border enforcement and international cooperation. The country's approach aligns with broader EU initiatives on AI governance and digital rights, potentially facilitating harmonized enforcement mechanisms across member states.[59] India faces greater challenges in international enforcement due to the territorial limitations of its current legal framework. While Indian courts have demonstrated a willingness to address cross-border digital identity violations, the lack of international treaties specifically addressing deepfakes and the limited scope of existing mutual legal assistance agreements constrain enforcement capabilities against foreign-hosted content or perpetrators located outside Indian jurisdiction.

The table below presents a comparative analysis of the legal frameworks governing deepfake regulation in Denmark and India.

Table 1: Comparative Legal Framework Analysis - Denmark vs. India

Aspect	Denmark	India
Primary Legal Basis	Copyright Act (Sections 73a & 65a)	Fragmented approach: Constitution (Art. 21), IT Act, IPC
Scope of Protection	Comprehensive biometric characteristics (face, voice, body)	Limited to specific harms (privacy, defamation, obscenity)
Consent Requirements	Mandatory prior written consent for all deepfake creation/distribution	No unified consent framework; case-by-case judicial interpretation
Post-mortem Protection	50 years after death	Not specifically addressed
Enforcement Timeline	Clear takedown procedures (specific timelines)	No standardized timelines; varies by legal provision
Platform Liability	Clear obligations with defined procedures	Uncertain; relies on existing IT Act safe harbour provisions
Penalties	Copyright infringement remedies damages	Varies: ₹2-10 lakh fines, 3-5 years' imprisonment (specific sections)
International Coordination	EU integration, harmonized standards	Limited bilateral agreements, territorial constraints
Legislative Status	Enacted in 2025, operational	No specific deepfake legislation
Fair Use/Exceptions	Explicit parody and satire protections	Judicial balancing on a case-by-case basis

5.2. Legal and Societal Impacts

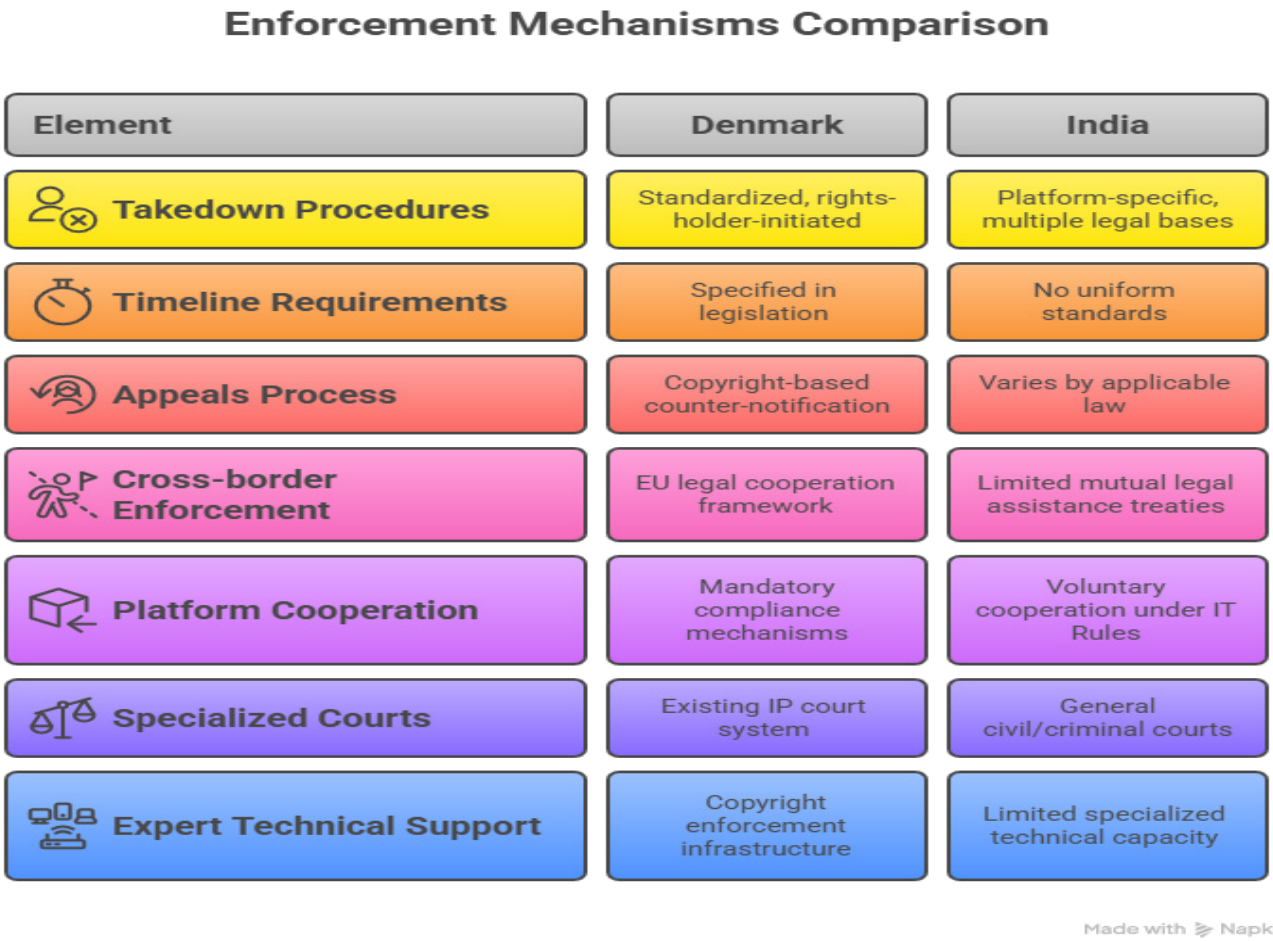
- **Individual Empowerment and Rights Protection:**Denmark's approach directly empowers individuals by granting them ownership rights over their biometric characteristics, creating a legal foundation for both preventive and remedial action against unauthorized deepfake use.[60] The Indian approach, while providing some protection through personality rights jurisprudence, places greater emphasis on judicial interpretation and case-by-case determinations of rights, creating uncertainty for individuals seeking protection.

- **Platform Responsibility and Industry Impact:**The Danish model establishes clear obligations for digital platforms and content creators, providing specific guidance about consent requirements and takedown procedures. This clarity benefits both rights holders and industry stakeholders by creating predictable legal boundaries and compliance requirements.[61] India's fragmented approach creates challenges for platform operators and content creators who must navigate multiple, potentially overlapping legal requirements without clear guidance specific to deepfake content.

- **Balancing Innovation and Protection:**Denmark's consent-based model attempts to balance individual rights and innovation by allowing authorized uses while restricting unauthorized exploitation. The inclusion of exceptions for parody and satirical content demonstrates sensitivity to free expression concerns.[62] India's approach relies more on judicial balancing of competing interests, with courts determining, on a case-by-case basis, how to reconcile personality rights with freedom of expression and technological innovation.

The figure below presents a comparative overview of the enforcement frameworks governing deepfake regulation in Denmark and India.

Figure 1: Comparative Enforcement Mechanisms for Deepfake Regulation in Denmark and India



POLICY RECOMMENDATIONS FOR INDIA

6.1. Legislative Amendments and Copyright Reform

India should introduce specific amendments to the Copyright Act, 1957, to create a robust, Denmark-inspired legal foundation for digital identity protection:

- **Proposed Section 73A (Biometric Likeness Protection):** Insert a provision protecting a natural person's physical characteristics (face, voice, body, gestures) from realistic digitally generated imitation without prior written consent. The rights should be inheritable and subsist for fifty years post-mortem.
- Definition: "Realistic digitally generated imitation" must be defined as AI-created content that substantially replicates a person's appearance or voice with sufficient accuracy to mislead a reasonable person.
- **Proposed Section 65A (Performer Protection):** Introduce specific protection for performers, ensuring realistic digitally generated imitations of their artistic performance, voice, or style cannot be made public without their consent. This consent should be withdrawable at any time.

6.2. Procedural Frameworks and Enforcement

The legal reform must be supported by precise procedural and regulatory mechanisms to ensure rapid and effective implementation:

- **Mandatory Consent Framework:** Establish comprehensive requirements for explicit, informed, and written consent for the creation and distribution of deepfakes. This framework must include standards for consent documentation and precise, rapid withdrawal mechanisms.
- **Balancing Legitimate Uses:** The consent requirements must be balanced through clearly defined exceptions, including:
- Fair Use Exceptions for educational, news reporting, academic, and artistic expression.
- Specific protections for Parody and Satire.
- Carefully crafted Public Interest Provisions.
- **Platform Responsibility and Rapid Response:** Establish a framework for platforms, including:
- Clear Takedown Procedures with differentiated timelines (e.g., shorter for electoral content).
- Balanced Notice and Counter-Notice Systems.
- Specific Platform Liability Standards that balance accountability with safe harbor protections.
- **Digital Identity Protection Authority (DIPA):** Consider establishing a specialized authority for:
- Coordinating enforcement across different legal frameworks.
- Developing Technical Standards for detection and authentication.
- Serving as the primary contact for international cooperation.

6.3. Alignment and International Cooperation

India's framework must guarantee compatibility with the global digital landscape.

- Global Standards Alignment: Ensure Indian law facilitates cooperation with EU enforcement mechanisms and aligns with the EU's leadership in AI governance.
- International Treaties: Develop specific provisions for Bilateral Cooperation Agreements and Mutual Legal Assistance in deepfake cases.
- Convention Compliance: Ensure the copyright-based approach aligns with India's obligations under the TRIPS Agreement and international Human Rights Conventions regarding freedom of expression.

CONCLUSION

This comparative analysis demonstrates a fundamental divergence in legal approaches to deepfake regulation. Denmark's pioneering legislation, which grants individuals copyright over their biometric likeness (Sections 73a and 65a), represents a paradigm shift toward proactive, rights-based protection built on precise consent mechanisms. This model offers compelling advantages in legal clarity, enforcement precision, and individual empowerment, surpassing reactive, litigation-dependent approaches. In contrast, India's fragmented legal landscape relies on constitutional rights and the IT Act, leading to inconsistencies, enforcement challenges, and uncertainty for rightsholders.

[60] Supra at 23.

[61] N. V. Munkholm and C. H. Schjøler, "Platform work and the Danish Model—legal perspectives" NJCL 116 (2018).

[62] "Denmark digital identity & copyright deepfakes," CryptoVerse Lawyers (2025), https://www.cryptoverselawyers.io/denmark-digital-identity-copyright-deepfakes/

The comparative findings underscore the urgent need for a unified statutory framework in India to address the complexities of AI-generated identity theft. The success of Denmark's approach provides a robust blueprint for global jurisdictions, including India. For India to enhance digital identity protection, the adoption of copyright-based personality rights is essential, which requires amending the Copyright Act (Proposed Sections 73A and 65A) and establishing a comprehensive consent-based framework. Successful adaptation necessitates careful calibration to India's unique constitutional structure and legal traditions, alongside the creation of a specialized regulatory body and the strengthening of cross-border enforcement mechanisms to manage the global nature of AI-generated content. The challenge of deepfake regulation ultimately reflects the fundamental test of existing legal institutions against rapidly evolving technology. The intersection of AI governance with human dignity requires continued legal innovation. Future research should focus on the practical impact of Denmark's enacted legislation and the development of effective international cooperation mechanisms. The ultimate goal remains achieving a careful balance between individual autonomy, technological advancement, and democratic governance in the twenty-first century.