DEEPFAKES AND THE RIGHT TO REPUTATION: A COMPARATIVE ANALYSIS OF INDIAN AND EUROPEAN LAW

Kashish Garg**,** Amity Institute of Advanced Legal Studies, Noida

ABSTRACT

The rapid advancement of generative artificial intelligence has made it easier to make deepfakes, which are created images, movies, and audio that can appear extremely real. Misuse of this content can have major ramifications for a person's reputation, dignity, privacy, and identity. This paper investigates the legal issues raised by deepfakes in regard to the right to reputation, with a specific emphasis on Indian law and a comparative analysis of the European Union's approach.

The paper examines current Indian laws, such as the Information Technology Act of 2000, the Bhartiya Nyaya Sanhita of 2023, and pertinent intermediate rules, that may be used to mitigate the negative effects of deepfakes. It also looks at how Indian courts are increasingly recognizing personality rights, especially when it comes to issues involving celebrities. The name, image, voice, likeness, and other distinguishing characteristics of popular persons have been increasingly shielded against unauthorized use and exploitation by courts, particularly the Delhi High Court. Despite these advancements, India still lacks a coherent legal framework that addresses deepfakes specifically, therefore protection is dispersed among several laws and judicial remedies.

In order to understand how the EU handles issues of transparency, platform responsibility, and AI-generated content, the study contrasts this stance with the framework of the EU, including the General Data Protection Regulation, Digital Services Act, and Artificial Intelligence Act. The study examines whether India's current legal framework is adequate to address the escalating threat of deepfakes and what can be learned from the EU strategy through a doctrinal and comparative examination. In the end, it makes the case for a more cohesive Indian framework that upholds the rights to one's character and personality while striking a balance with freedom of speech and technological advancement.

Keywords: Deepfakes, Right to Reputation, Personality Rights, Artificial Intelligence, Privacy, Indian Legal Framework, European Union

1. Introduction

The advent of deepfake technology has made reputation protection in the digital sphere more difficult. AI-generated or AI-manipulated photos, videos, or audio recordings that can accurately portray a human saying or doing something that never happened are known as deepfakes. Their legal significance stems not only from the presence of modified material but also from how simple it is to make, replicate, and disseminate it widely. Deepfakes can directly harm a person's reputation and dignity when they are used to fraudulently link them to criminal action, sexual activity, insulting remarks, or other socially harmful behaviour.

The problem exposes a gap between technological development and existing legal remedies. Identifiable acts of publication and comparatively common forms of false representation were the main focus of the development of traditional defamation laws. These presumptions are complicated by deepfakes. A manipulated video's creator may remain unknown, it may be challenging to identify the individual who first published it, and users and platforms in many jurisdictions may regularly replicate the content. It's possible that the content has already been replicated and shared on several sites by the time a victim learns about it and requests its removal. This poses a crucial legal question: can current defamation, privacy, personality rights, data protection, and intermediary liability standards effectively protect against reputational damage brought on by AI-generated content?

The Indian legal framework does not presently provide a single, comprehensive legal regime specifically addressing deepfake-related harm to reputation. Protection may instead be sought through several overlapping areas of law. The constitutional recognition of reputation as an aspect of Article 21 provides an important foundation for protecting an individual's reputation[1], while civil and criminal defamation provide conventional remedies against false statements that harm reputation.[2] The Information Technology Act, 2000[3] and rules governing intermediaries[4] also become relevant where manipulated content is disseminated through online platforms. In addition, privacy and personality rights recognised through judicial decisions may provide further protection in appropriate cases. However, the application of these existing laws to deepfakes raises questions concerning attribution, intermediary

[1] Subramanian Swamy v. Union of India, (2016) 7 SCC 221.
[2] The Bharatiya Nyaya Sanhita 2023 § 356.
[3] The Information Technology Act 2000.
[4] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, as amended in 2026.

responsibility, speed of removal, jurisdiction, and the distinction between unlawful manipulation and legitimate forms of expression.

The European legislative framework provides a varied regulatory context. The European Union has created a more comprehensive framework for governing digital platforms, personal data, and artificial intelligence. The General Data Protection Regulation provides protection in relation to the processing of personal data[5], while the Digital Services Act establishes obligations for online platforms concerning illegal content and systemic risks.[6] More recently, the EU Artificial Intelligence Act has introduced specific transparency obligations concerning certain AI-generated or manipulated content, including deepfakes.[7] Because of these developments, European law is especially pertinent for analysing whether a regulatory strategy that incorporates platform obligations, data protection, individual rights, and AI-specific regulation may offer more effective protection against reputational harm.

Therefore, it is important to compare India and Europe not just because both countries govern developing technologies but also because they use different legal frameworks to address the interplay between individual rights, technical innovation, and platform responsibility. While the European Union has moved toward a more comprehensive regulatory framework for digital platforms and artificial intelligence, India mostly addresses the issue through a combination of constitutional protections and current statute and judicial remedies. The comparison offers a chance to assess if the current legal safeguards in India are sufficient in light of deepfakes and whether elements of the European regulatory approach could guide the creation of an efficient Indian framework.

The central concern of this research is therefore the adequacy of legal protection available to an individual whose reputation is harmed by a deepfake. The study examines how the right to reputation is understood and protected in India and Europe, the applicability of existing defamation and privacy principles to deepfake content, and the extent of liability that may be imposed on creators, distributors, and online intermediaries. It further examines how the law balances protection of reputation against freedom of speech and expression, particularly where manipulated content may have artistic, satirical, journalistic, or political purposes.

[5] Regulation (EU) 2016/679, 2016 O.J. (L 119) 1 (EU).
[6] Regulation (EU) 2022/2065, 2022 O.J. (L 277) 1 (EU).
[7] Regulation (EU) 2024/1689, art. 50, 2024 O.J. (L) (EU).

This study compares Indian and European law in an effort to determine the shortcomings of the current Indian framework and determine whether the European approach provides helpful guidelines for dealing with reputational damage caused by deepfakes. In the end, the study examines whether India needs special laws and regulations to cope with deepfakes or whether the right to reputation in the era of artificial intelligence may be sufficiently protected by current legal principles provided they are properly interpreted and upheld.

2. Statement of Problem

The growing usage of deepfake technology has posed a significant problem to protecting an individual's reputation. AI-generated and manipulated content can erroneously portray people as participating in behaviour that could harm their personal, social, or professional status, while the speed and scope of internet dissemination make effective legal remedies impossible to achieve. The situation is exacerbated by concerns about the responsibility of producers, users, and internet intermediaries, as well as the need to defend legitimate freedom of expression.

In India, there is no comprehensive legal structure that addresses deepfakes and their influence on reputation. Although current laws governing defamation, privacy, personality rights, and intermediary responsibility may provide some remedies, their effectiveness in dealing with the unique nature of deepfake-related harm is unknown. In contrast, the European Union has devised particular legal measures to handle AI-generated content in addition to broader protections for privacy, data, and digital rights. The challenge is to assess whether existing legal frameworks in India and Europe give enough and effective protection against reputational harm caused by deepfakes, and whether the European approach provides valuable legal principles for upgrading the Indian system.

3. Research Questions

1. To what extent does the existing Indian legal framework protect an individual's right to reputation against harm caused by deepfakes?
2. How does the European legal framework address deepfake-related harm and how does it compare with the Indian position?
3. What legal and regulatory measures can India adopt, drawing from the European approach, to provide effective protection against deepfake-related reputational harm?

4. Research Objectives

1. To examine the existing Indian legal provisions and judicial principles relating to defamation, privacy, personality rights, and intermediary liability, and assess their applicability and effectiveness in protecting individuals from reputational harm caused by deepfakes.
2. To analyse the European legal framework governing deepfakes and reputational harm, with particular focus on data protection, privacy and personality rights, intermediary liability, and AI-specific regulation, and to compare these protections with the corresponding Indian legal framework.
3. To identify the gaps and limitations in the Indian legal framework and examine the extent to which relevant principles and regulatory measures from the European framework can be adapted to strengthen legal protection against deepfake-related reputational harm in India.

5. Research Methodology

The present study adopts a doctrinal and comparative legal research methodology to examine the protection of the right to reputation against deepfake-related harm under Indian and European law. The research is qualitative in nature and primarily relies on the analysis and interpretation of existing legal and academic materials.

The doctrinal component examines primary legal sources, including the Constitution of India, statutes, judicial decisions, regulations, and other relevant legal instruments concerning defamation, privacy, personality rights, intermediary liability, data protection, and artificial intelligence. Secondary sources, including books, journal articles, research papers, legal commentaries, policy reports, and institutional publications, are also examined to understand the existing academic discourse on deepfakes and reputational harm.

The comparative component analyses the Indian legal framework alongside the European framework, with particular focus on data protection, privacy and personality rights, intermediary regulation, and AI-specific legislation. Relevant judicial decisions are analysed to understand the development of the right to reputation and related protections in cases involving digitally manipulated or disseminated content. The study identifies similarities,

differences, gaps, and limitations in the two frameworks and uses these findings to assess the adequacy of Indian law and suggest possible legal and regulatory measures for strengthening protection against deepfake-related reputational harm.

6. Research Hypothesis

The current Indian legal framework, which protects against reputational harm through defamation, privacy, personality rights, and intermediary responsibility, is insufficient to address the unique issues created by deepfakes. A comparative analysis of the European legal framework is expected to show that a more precise and coordinated legislative and regulatory strategy is required in India to effectively protect the right to reputation from deepfake-related harm.

7. Literature Review

The advancement of generative artificial intelligence has led to a significant expansion of legal scholarship on deepfakes. Early research focused mostly on deepfakes as a danger to national security, democratic processes, privacy, and reputation. The focus of more recent writing has shifted to issues of AI regulation, intermediary liability, personality rights, and the suitability of current legal remedies. However, little is known about the precise connection between deepfakes and the right to reputation, especially when comparing Indian and European legislation.

One of the foundational works in this area is Robert Chesney and Danielle Keats Citron's analysis of deepfakes in their article “Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security”.[8] While highlighting the challenge of reacting to content that can be created and shared quickly and widely, they identify deepfakes as a technological advancement capable of causing serious individual harms, such as personal sabotage, exploitation, and reputational harm. Their work is especially significant since it shows that technological solutions are insufficient to solve the issue and that legal culpability and regulatory measures must be taken into account.

[8] Robert M. Chesney and Danielle Keats Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security,* 107 CALIFORNIA LAW REVIEW (2019).

The European regulatory approach has received increasing attention following the adoption of the EU Artificial Intelligence Act. Mateusz Łabuz, in his research article titled "Deep fakes and the Artificial Intelligence Act—An important signal or a missed opportunity?"[9], examines the treatment of deepfakes under the AI Act and argues that the legislation represents an important regulatory development because it introduces transparency obligations for certain AI-generated or manipulated content. At the same time, he identifies limitations in the framework, particularly because not all forms of deepfake content receive the same degree of regulatory protection.

Indian scholarship has increasingly focused on the inadequacy of existing legal mechanisms in addressing deepfakes. Shinu Vig examines the Indian regulatory framework and considers the possible application of intellectual property, criminal law, and privacy law to deepfake-related harms. Vig, in her article titled "Regulating Deepfakes: An Indian Perspective"[10], concludes that although existing laws can address certain aspects of the problem, India requires more specific legal and regulatory measures to deal with synthetic media.

Recent Indian scholarship has also increasingly connected deepfakes with personality rights and identity protection. Sonu Shaji examines India's existing legal framework concerning deepfakes and personality rights in her article "Legal Framework Governing Deepfake & Personality Rights in India: A Critical Analysis"[11] and argues that constitutional protections, tort principles, and the Information Technology Act provide only partial protection. The study highlights the absence of a dedicated statutory framework and the resulting dependence on judicial development.

Jeeva Chacko's recent work titled "Cloning the Persona: Personality and Publicity Rights in the Age of AI Deepfakes and Voice Cloning in India"[12] takes this discussion further by examining the development of personality and publicity rights in India in the context of AI deepfakes and voice cloning. The study traces the judicial development of protection for name, image, voice, mannerisms, and other elements of personal identity and highlights the absence of a dedicated statutory framework. It also identifies uncertainty regarding the scope of

[9] Mateusz Łabuz, *Deep Fakes and the Artificial Intelligence Act: An Important Signal or a Missed Opportunity?,* 16 POLICY & INTERNET (2024).
[10] Shinu Vig, *Regulating Deepfakes: An Indian Perspective,* 17 JOURNAL OF STRATEGIC SECURITY (2024).
[11] Sonu Shaji*, Legal Framework Governing Deepfake & Personality Rights in India: A Critical Analysis*, 6 INDIAN JOURNAL OF LEGAL REVIEW (2026).
[12] Jeeva Chacko, *Cloning the Persona: Personality and Publicity Rights in the Age of AI Deepfakes and Voice Cloning in India,* 2 INDIAN JOURNAL OF JURISPRUDENCE AND REVIEWS (2026).

protection and the distinction between celebrity rights and protection available to ordinary individuals.

Further, Abhishek Kukreti, Vivek Kumar, and Avishek Raj provide a cross-jurisdictional examination of deepfakes, copyright, and personality rights across India, the United States, and the European Union. Their analysis in their research article "Deepfakes, Copyright, and Personality Rights: A Cross-Jurisdictional Analysis"[13] identifies shortcomings in existing legal frameworks and emphasises the need to reconsider existing approaches to defamation, privacy, and personality rights in light of digital manipulation.

Finally, the emerging Indian literature specifically addressing deepfake-related reputational harm indicates that the issue is no longer limited to privacy or intellectual property. Recent scholarship has begun to examine deepfakes as a direct threat to reputation and identity, particularly in the context of celebrity rights and unauthorised digital representations. Pragya Sharma and Payodhi Daschaudhuri, for example, in their research article titled "Synthetic Faces, Real Disrepute: Deepfake and the Quest to Safeguard Celebrity Rights and Reputation"[14] examine the impact of deepfakes on celebrity identity and reputation and highlight the limitations of existing legal mechanisms in protecting these interests.

7.1 Research Gap Emerging from the Literature Review

Although existing literature has examined deepfakes in relation to privacy, defamation, personality rights, intermediary liability, and AI regulation, there is limited research that specifically examines deepfakes as a threat to the right to reputation from a comparative India-Europe perspective. Indian scholarship largely addresses deepfakes through fragmented areas of law, while European scholarship has increasingly focused on AI-specific and platform regulation. However, the adequacy of these frameworks in providing an effective remedy for deepfake-related reputational harm has not been sufficiently compared. This study seeks to fill this gap by comparatively analysing the Indian and European legal frameworks, identifying the limitations of Indian law, and examining possible legal and regulatory measures for strengthening protection of reputation in India.

[13] Abhishek Kukreti, Vivek Kumar and Avishek Raj, *Deepfakes, Copyright, and Personality Rights: A Cross-Jurisdictional Analysis,* 5 JOURNAL OF INFORMATICS EDUCATION AND RESEARCH (2025).
[14] Pragya Sharma and Payodhi Daschaudhuri, *Synthetic Faces, Real Disrepute: Deepfake and the Quest to Safeguard Celebrity Rights and Reputation,* 2 JOURNAL OF LEGAL RESEARCH AND POLITY (2025).

8. Indian Legal and Judicial Analysis

India does not presently have a single, dedicated statute governing deepfakes and their impact on reputation. Instead, protection is distributed across constitutional law, defamation law, privacy and personality rights, information technology legislation, and intermediary regulation. This fragmented structure is essential to the current study because a deepfake might simultaneously involve many legally protected interests, while the appropriate remedy may vary depending on the nature of the modified content and how it is disseminated.

8.1 Constitutional Protection of Reputation

In India, the analysis of reputational harm begins with Article 21 of the Constitution, which safeguards the right to life and personal liberty.[15] The Supreme Court has explicitly acknowledged reputation as a component of this right. In *Subramanian Swamy v. Union of India*[16], the Hon'ble Court upheld the constitutionality of criminal defamation and viewed reputation as an essential component of an individual's dignity and personality. The Court also recognised that the protection of reputation must be considered alongside freedom of speech and expression under Article 19(1)(a).

This constitutional recognition is especially crucial for deepfakes. A fabricated video, image, or audio recording that falsely attributes criminal, immoral, or otherwise detrimental behaviour to a person can harm not just their public image, but also their dignity, social ties, and professional status. Even though Article 21 does not specify a precise remedy, the constitutional protection of reputation serves as a vital normative underpinning for dealing with deepfake-related harms.[17]

The challenge, however, is turning this fundamental guarantee into an effective remedy against digitally generated content. Article 21 recognizes the importance of reputation as a protected interest, but in most cases, the victim must rely on other areas of law, such as defamation, privacy, personality rights, or information technology law, to obtain practical relief.

[15] INDIAN CONST. art 21.
[16] *Supra* note 1.
[17] Asim Mustafa Khan, *Regulating Deepfakes in India: A Legal and Ethical Analysis of Misinformation in the Age of AI,* 7 INDIAN JOURNAL OF LAW AND LEGAL RESEARCH 7652 (2025).

8.2 Defamation and Deepfakes

Defamation remains one of the most obvious legal routes where a deepfake falsely depicts an individual in a manner that lowers their reputation. Following the replacement of the Indian Penal Code by the Bharatiya Nyaya Sanhita, 2023 (BNS), defamation is now governed principally by Section 356. The provision covers imputations made through words, signs, or visible representations, where the person making or publishing the imputation intends, knows, or has reason to believe that it will harm another person's reputation.[18]

The term "visible representations" is significant in the context of deepfakes. Even if no conventional written or spoken defamatory statements are present, a modified video or image may constitute an imputation. The BNS thus establishes a conceptual foundation for applying defamation principles to specific types of deepfake content.

However, traditional defamation law has several restrictions. The victim may need to prove that the text contains an identifiable imputation about them and that the publication is capable of hurting their reputation. Deepfake technology challenges issues of authorship, publication, intention, identifying the person responsible, and attribution of content. An anonymous creator may be difficult to track down, whereas a deepfake can be published thousands of times by people who did not make it.

There is also a gap between the substantive availability of defamation law and its practical application in the deepfake context. Section 356 can potentially address the harm, but it was not specifically designed for AI-generated representations capable of instantaneous and repeated dissemination.

8.3 Civil Remedies and Protection of Reputation

Apart from criminal defamation, a person can seek civil remedies for reputational harm, such as damages and injunctive relief. Injunctions are especially important in deepfake cases, when monetary compensation after widespread diffusion may not be sufficient to remedy the harm.

[18] *Supra* note 2.

The Delhi High Court's ruling in *Anil Kapoor v. Simply Life India & Ors.*[19] is an important example. The Court awarded protection for the actor's name, image, likeness, voice, persona, and other personality traits, and particularly prohibited misuse using technological tools such as AI, machine learning, deepfakes, and face morphing. The Court acknowledged that such usage could jeopardize privacy, dignity, livelihood, and reputation, and ordered the removal of identified infringing materials.

The decision is especially noteworthy for the present research because it shows that Indian courts can employ existing civil and personality-rights principles to address technologically induced misuse even in the lack of a specialized deepfake statute. At the same time, the case addressed a well-known celebrity with established personality rights. This poses a crucial question for the broader legal framework: whether ordinary individuals who suffer reputational injury as a result of deepfakes but lack commercially valuable or judicially recognized personality rights have comparable access to similar protection.

8.4 Privacy and Personality Rights

Deepfakes may also violate privacy and personality interests by reproducing a person's face, voice, picture, name, or other identifying attributes without consent. The Indian judiciary has evolved personality rights primarily through a combination of privacy, publicity, passing off, intellectual property, and constitutional principles, rather than a single statutory right.

This judicial development is especially significant since a deepfake does not always have to include a defamatory allegation to create legal harm. A sexually explicit fabricated video, for example, may substantially harm an individual's privacy and dignity even if the content does not meet all of the criteria for defamation. Similarly, even in the absence of an express defamatory comment, the unauthorized use of a person's voice or likeness may constitute an infringement of personality interests.

The *Anil Kapoor* decision exemplifies the scope of this new judicial paradigm. The Delhi High Court safeguarded some aspects of the plaintiff's persona and expressly identified the use of AI and deepfake technology as a forbidden misuse.

[19] Anil Kapoor v. Simply Life India & Ors., 2023 SCC OnLine Del 6914.

Nonetheless, personality rights protection in India is primarily judge-made and scattered. There is no comprehensive statutory structure outlining the scope, duration, beneficiaries, limitations, and remedies for personality rights. This is especially problematic when deepfake technology replicates a person's identity without actually copying a traditional copyrighted work.

8.5 Information Technology Act, 2000

The Information Technology Act of 2000 adds another degree of protection. Although the Act does not include a particular offense known as "deepfake," numerous prohibitions may become applicable based on the content and circumstances. These include provisions dealing with identity theft under Section 66C[20], cheating by personation under Section 66D[21], privacy violations under Section 66E[22], and sexually explicit or obscene material under Sections 67[23] and 67A[24]. Section 69A[25] also provides a mechanism for restricting public access to specific internet material.

The challenge is that these prohibitions are content- and conduct-specific rather than technology-specific. A deepfake may be an offense under one of these clauses in some cases but not in others. For example, a fabricated video that harms someone's professional reputation but is neither sexually explicit nor utilized for cheating may not fall neatly within Sections 66C, 66D, or 67.

As a result, the IT Act supplemented rather than replaced defamation, privacy, and personality-rights remedies. Its scattered implementation exemplifies one of our research's main concerns: Indian law can address certain manifestations of deepfake harm, but it does not yet provide a cohesive legal framework based on the unique hazards posed by synthetic media.

8.6 Intermediary Liability and the IT Rules

Online platforms play an important role since the harm caused by a deepfake is often determined by its spread and amplification rather than its production. Section 79 of the IT Act[26]

[20] *Supra* note 3, § 66C.
[21] *Supra* note 3, § 66D.
[22] *Supra* note 3, § 66E.
[23] *Supra* note 3, § 67.
[24] *Supra* note 3, § 67A.
[25] *Supra* note 3, § 69A.
[26] *Supra* note 3, § 79.

provides intermediaries with conditional safe harbour if they meet certain standards. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021[27] place additional due diligence requirements on intermediaries.

India's regulatory position has developed significantly in response to synthetic media. In December 2023, MeitY expressly directed intermediaries to ensure that users were clearly warned about illegal content under the IT Rules in relation to AI-generated misinformation and deepfakes.[28]

More importantly, India's 2026 revisions to the IT Rules included particular regulation of synthetically generated information (SGI).[29] The updated framework defines SGI and sets extra due diligence requirements for its creation, dissemination, labelling, and traceability. It also establishes stricter user-awareness standards and faster compliance duties for specific types of dangerous content.

This development significantly alters the Indian legal position and should be considered in any current research on deepfakes. The regulatory approach has evolved from relying exclusively on traditional defamation and cybercrime legislation to platform-level preventive and transparency requirements.

However, a significant constraint remains. The new framework governs synthetic content primarily via the intermediary and information-regulation architectures. It does not provide a separate statutory cause of action for protection against deepfake-related reputational harm. The victim may still have to rely on a variety of legal measures, depending on the nature of the harm.

8.7 Judicial Approach to Deepfake-Related Harm

Indian courts have increasingly evolved personality rights as a result of judicial rulings regarding the unauthorized use of an individual's name, picture, voice, likeness, and other characteristics of their persona. Although there is no complete statutory framework governing

[27] *Supra* note 4.
[28] Ministry of Electronics & Information Technology, Government of India, *Due Diligence by Intermediaries and Grievance Reporting Mechanism, under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021* (Dec. 26, 2023).
[29] Ministry of Electronics & Information Technology, Government of India, *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026*, G.S.R. 120(E), Feb. 10, 2026.

personality rights or deepfakes, recent cases show that courts are increasingly applying these principles to AI-generated content.

i. D.M. Entertainment Pvt. Ltd. v. Baby Gift House[30]

The Delhi High Court acknowledged that a celebrity's identity has independent commercial value, and that unauthorized commercial exploitation of that identity may infringe publicity rights. Despite the fact that no AI or deepfakes were involved, the case laid a solid foundation for India's personality-rights law.

ii. Titan Industries Ltd. v. Ramkumar Jewellers[31]

The Delhi High Court upheld the unauthorized commercial use of Amitabh Bachchan and Jaya Bachchan's images in advertisements. The verdict strengthened recognition of publicity rights while also demonstrating the limitations of relying on passing-off and commercial exploitation rules in cases when deepfakes inflict only reputational harm.

iii. Amitabh Bachchan v. Rajat Nagi[32]

The Delhi High Court awarded protection against unauthorized use of Amitabh Bachchan's name, image, voice, likeness, and other aspects of his persona. The ruling is noteworthy because it demonstrates that personality rights go beyond a person's portrait and can include a variety of distinguishing qualities.

iv. Jaikishan Kakubhai Saraf v. The Peppy Store & Ors.[33]

The Delhi High Court recognized protection for Jackie Shroff's name, image, voice, likeness, mannerisms, and distinguishing characteristics. The example is significant because it highlights how personality can expand beyond visual identification to include traits that distinguish an individual.

[30] D.M. Entertainment Pvt. Ltd. v. Baby Gift House, 2010 SCC OnLine Del 4790.
[31] Titan Industries Ltd. v. Ramkumar Jewellers, 2012 SCC OnLine Del 2382.
[32] Amitabh Bachchan v. Rajat Negi, (2022) 6 HCC (Del) 641.
[33] Jaikishan Kakubhai Saraf v. The Peppy Store & Ors., 2024 SCC OnLine Del 3664.

v. Arijit Singh v. Codible Ventures LLP[34]

The Bombay High Court granted protection against the unauthorized use of Arijit Singh's voice and character via AI-based voice cloning and related technologies. The decision is especially pertinent to deepfakes because it acknowledges voice as an important and protectable aspect of personal identification.

vi. Aishwarya Rai Bachchan v. Aishwaryaworld.com & Ors.[35]

The Delhi High Court addressed the unauthorized use of Aishwarya Rai Bachchan's name, image, likeness, and other personality traits using AI and deepfakes. The ruling highlights the growing use of judicial injunctions and takedown mechanisms to give meaningful protection against digitally transmitted personality-related harm.

These rulings clearly show a shift from preserving the commercial value of celebrity identification to safeguarding a broader range of personality traits, such as voice and AI-generated representations. However, the jurisprudence is still mostly judge-made and celebrity-focused, raising questions about the protection provided to ordinary people whose reputations are injured by deepfakes. This constraint is especially pertinent to the present research, which investigates whether existing Indian law adequately protects the right to reputation, as opposed to only the commercial exploitation of personality.

9. Comparative Analysis of Indian and European Law on Deepfakes and Protection of Reputation

The legal regulation of deepfakes in India and the European Union takes two distinct approaches to protecting individuals from the harms caused by AI-generated and manipulated content. In India, protection is provided by a combination of constitutional protection of reputation and dignity, defamation law, privacy and personality rights, and intermediary

[34] Arijit Singh v. Codible Ventures LLP, 2024 SCC OnLine Bom 2445.
[35] Aishwarya Rai Bachchan v. Aishwaryaworld.com & Ors., 2025 SCC OnLine Del 5943.

regulation. The European Union, although relying on fundamental rights and existing privacy safeguards, has created a more comprehensive legislative framework through the General Data Protection Regulation (GDPR), the Digital Services Act (DSA), and the Artificial Intelligence Act (AI Act). These instruments function at various stages of the deepfake lifecycle and, collectively, provide a good comparison to the Indian framework.

In India, the right to reputation is recognized as part of Article 21 of the Constitution. In *Subramanian Swamy v. Union of India*[36], the Supreme Court recognized reputation as a vital component of an individual's dignity and upheld criminal defamation as a constitutionally legitimate limitation on free expression. This establishes the fundamental legal framework for defending an individual whose reputation has been injured by a deepfake. Section 356 of the Bharatiya Nyaya Sanhita, 2023,[37] which deals with defamation, is also applicable because it addresses imputations made through "visible representations." A manipulated image or video may consequently be considered defamatory if it wrongly attributes activity to an identifiable individual and causes reputational injury.

Individuals' identities and personas are likewise protected under Indian law through privacy and personality rights. The Supreme Court's ruling in *Justice K.S. Puttaswamy (Retd.) v. Union of India*[38] affirmed privacy as a fundamental right under Article 21, safeguarding human autonomy, dignity, and control over personal information. Indian courts have now created personality-rights doctrine to protect names, images, voices, likenesses, and other distinguishing features of an individual's identity. Decisions such as *D.M. Entertainment v. Baby Gift House*[39], *Anil Kapoor v. Simply Life India*[40], *Jackie Shroff v. The Peppy Store*[41], and *Arijit Singh v. Codible Ventures LLP*[42] show that these concepts can also apply to AI-generated photos, deepfakes, and voice cloning.

The European framework addresses the same issue with a more comprehensive combination of data protection, platform regulation, and AI-specific regulation. The GDPR[43] applies where the production or use of a deepfake requires the processing of personal data. Its framework gives individuals rights over the processing and use of their personal data and establishes

[36] *Supra* note 1.
[37] *Supra* note 2.
[38] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
[39] *Supra* note 30.
[40] *Supra* note 19.
[41] *Supra* note 33.
[42] *Supra* note 34.
[43] *Supra* note 5.

requirements on organizations that process such data. The GDPR's restrictions on special categories of personal data, such as biometric data processed for the aim of uniquely identifying a natural person, are particularly applicable.[44] Thus, while the GDPR does not establish a unique "right against deepfakes," it can provide an important layer of protection where deepfake development or dissemination contains identifiable personal or biometric data.

The GDPR is thus akin to India's constitutional privacy and growing personality-rights framework, but the two regimes differ significantly in structure. In India, judicial rulings have significantly shaped the protection of a person's appearance, voice, and likeness, which is nevertheless fragmented across many legal doctrines. In the EU, data protection is implemented through a precise statutory framework that includes defined rights, obligations, and enforcement mechanisms. The GDPR thus establishes a more organized method for controlling the processing of personal data that may be used to create or distribute synthetic representations.

The Digital Services Act[45] expands upon the European framework by addressing the role of online intermediaries and platforms. The DSA became legally binding for online intermediaries and platforms in August 2023, imposing due diligence responsibilities regarding illegal content, transparency, and systemic risks. Very Large Online Platforms and Search Engines are obligated to identify and minimize systemic hazards associated with their services.[46] The European Commission has highlighted malicious deepfakes and damaging AI-generated content as significant systemic concerns.

This is crucial for reputation protection since the harm produced by a deepfake is frequently determined by its amplification and diffusion across digital channels. A fabricated video may have little influence when viewed by a few people, but it can inflict significant reputational harm when algorithmically promoted, reposted, and viewed by millions. As a result, the DSA shifts the focus away from whether an individual creator is accountable and toward platforms' obligations in controlling systemic risks.

India also recognizes intermediary responsibility under Section 79 of the Information Technology Act[47] and the Information Technology (Intermediary Guidelines and Digital Media

[44] *Supra* note 5, art 9.
[45] *Supra* note 6.
[46] *Supra* note 6, arts 34-35.
[47] *Supra* note 26.

Ethics Code) Rules[48]. India's regulatory framework has progressively included requirements for synthetic media and deepfakes. However, the European approach is more clearly centred on platform-wide systemic risk assessment, transparency, and responsibility. This distinction is significant because successful reputation protection necessitates not only a remedy against the original creator, but also systems capable of preventing the ongoing spread of harmful content.

The EU Artificial Intelligence Act[49] represents the most significant difference between the two jurisdictions. Unlike traditional defamation or privacy laws, the AI Act explicitly recognizes deepfakes as a type of AI-generated or manipulated content. A deepfake is defined in Article 3(60)[50] as AI-generated or manipulated image, audio, or video content that resembles existing people, objects, locations, entities, or events that appears to a person to be legitimate or truthful.

Article 50[51] specifies transparency requirements for AI-generated material. Providers of AI systems that generate synthetic audio, images, video, or text must ensure that their outputs are machine-readable and identifiable as artificially generated or manipulated. Deployers of systems that generate or edit picture, audio, or video content to create a deepfake must disclose that the content was artificially generated or manipulated. The information must be presented in a clear and distinct manner no later than the initial exposure to the topic. These disclosure duties begin on August 2, 2026.

This is particularly crucial in terms of reputation. The primary risk posed by a deepfake is that the viewer may believe the created depiction is genuine. If a video incorrectly depicts someone making a defamatory speech or engaged in criminal behaviour, reputational damage may occur before the victim has a chance to seek legal redress. Article 50 aims to decrease the probability of synthetic content being misidentified as a real representation by requiring notification at the moment of exposure. As a result, the EU framework includes a preventive aspect that has not previously existed in defamation law.

The AI Act also requires vendors of generative AI systems to allow the detection of AI-generated or manipulated content via machine-readable tagging. This is significant because visible labels can be deleted when content is downloaded or replicated, whereas machine-readable provenance procedures can help platforms and technological systems detect fake

[48] *Supra* note 4.
[49] *Supra* note 7.
[50] *Supra* note 7, art 3(60).
[51] *Supra* note 7, art 50.

content. The EU's Code of Practice on Transparency of AI-Generated Content offers more practical recommendations on marking and labelling synthetic content.

At the same time, the AI Act does not consider every manipulated representation illegal. Article 50 provides exemption and reduced responsibilities for clearly artistic, creative, satirical, fictitious, or analogous works. In such circumstances, disclosure must be made in an acceptable manner that does not interfere with the presentation or enjoyment of the work. This approach is significant because it reveals that the European framework aims to distinguish between false synthetic content and legitimate creative applications, rather than just eliminating modified content.

This aspect provides an important lesson for India. A legislative framework dealing with deepfakes must avoid labelling all AI-generated or modified content illegal. A satirical video, fictitious film, parody, or creative piece may contain manipulation without resulting in legally actionable reputational harm. What requires further control is content that is presented or seen to be legitimate and causes or is likely to cause identifiable harm.

As a result of the comparison, the two systems give significantly different types of legal protection. Indian law primarily offers rights-based and remedial protection. Individuals who have had their reputations injured can seek damages for defamation, privacy, personality rights, and injunctions, whereas platforms are held to intermediary requirements. The European approach adds a more robust preventive and regulatory layer, mandating AI providers to aid detection, deployers to disclose deepfakes, and big internet platforms to address systemic threats.

However, the European framework does have limitations. The AI Act's disclosure standards do not constitute a comprehensive cause of action for reputational harm. Labelling a deepfake does not necessarily compensate the victim or delete defamatory content. Even if a person's reputation has already been harmed, they may still be required to abide by applicable national civil, criminal, or privacy laws. Similarly, the GDPR focuses on personal data rather than reputation as an independent legal interest. The power of the European approach is thus found not in a single statute, but in the combined operation of the GDPR, DSA, and AI Act.

10. Findings, Suggestions and Conclusion

10.1 Findings:

The study concludes that deepfakes pose a significant threat to the preservation of the right to reputation since they can construct very convincing but entirely fabricated representations of an individual. Deepfakes, unlike traditional defamatory material, may mimic a person's face, voice, expressions, and habits, making it impossible for viewers to tell the difference between legitimate and manipulated content. Their quick and frequent broadcast via digital channels raises the risk of substantial and ongoing reputational harm.

The analysis of Indian law reveals that the country has legal systems in place to deal with this kind of injury. While defamation law offers a remedy against false accusations that could damage one's reputation, Article 21 of the Constitution offers a constitutional basis for the protection of reputation and dignity. Aspects of an individual's identity, such as their name, picture, likeness, and voice, are further protected under privacy and personality rights doctrine. Indian courts are willing to apply these principles to AI-generated content, deepfakes, and voice cloning, as seen by recent court rulings like *Anil Kapoor v. Simply Life India, Jaikishan Kakubhai Saraf v. The Peppy Store, and Arijit Singh v. Codible Ventures LLP*.

The study discovers that these safeguards are still dispersed, nevertheless. There isn't a single, all-encompassing legal framework that addresses reputational harm caused by deepfakes. Depending on whether the harm includes defamation, privacy, personality rights, identity theft, sexually explicit content, or unauthorised commercial exploitation, the victim may need to rely on various legal provisions. This may raise questions about the proper course of action and the responsibility of various parties involved in the production and distribution of deepfakes.

The analysis also reveals that, despite being progressive, Indian personality-rights law has mostly evolved as a result of instances involving celebrities and commercial exploitation. This calls into doubt the protection afforded to common people whose identities lack established commercial value but whose reputations are severely harmed by deepfakes. Therefore, it is still crucial to distinguish between the more general right to reputation and commercial personality rights.

The European Union offers a more structured regulatory framework. The GDPR protects individuals who create or use deepfakes that entail the processing of personal data, whereas the Digital Services Act addresses the duties of intermediaries and platform providers. The EU Artificial Intelligence Act takes a step further, explicitly regulating AI-generated and modified content and establishing transparency requirements for deepfakes. The European framework thus augments traditional legal remedies with preventive and regulatory initiatives.

The study concludes that the combined effect of the GDPR, DSA, and AI Act is the main strength of the EU approach rather than any one piece of law. These tools tackle several facets of the issue, such as transparency, platform accountability, identification of synthetic material, and personal data. However, because victims may still need to rely on relevant national laws pertaining to defamation, privacy, and personality rights, the EU framework does not offer a comprehensive remedy for reputational harm.

Overall, the comparative analysis shows that while Indian law offers a strong basis for reputation protection, it lacks the level of coordination and technology-specific regulation seen in the European framework.

10.2 Suggestions:

According to the study's conclusions, the following measures could strengthen India's legal reaction to reputational injury caused by deepfakes:

i. Create a comprehensive framework for deepfakes

India should consider creating a legal framework for dealing with deepfakes and other forms of synthetic media. Such a framework does not have to replace existing defamation, privacy, and personality-rights laws. Instead, it should specify how existing remedies apply to AI-generated information and impose precise requirements for its creation and dissemination.

ii. Strengthen mandatory labelling of deepfake content

Article 50 of the EU AI Act can be used by India to mandate that artificial intelligence (AI)-produced or altered audio, images, and videos that seem authentic must clearly and conspicuously disclose that they are artificially generated or manipulated. When the content is initially made accessible to users, the disclosure ought to be given.

This would immediately address the potential for viewers to mistake a fake representation for the real thing, which is one of the main sources of reputational damage.

iii. Strengthen intermediary responsibility

Using the Digital Services Act, India could impose clearer requirements on key digital platforms regarding deepfake-related dangers. Platforms should have adequate processes in place to receive complaints, validate reported deepfakes, preserve relevant evidence, and

respond quickly to content that is illegal or causes substantial and verifiable harm.

The responsibilities should go beyond just responding to individual complaints. Major platforms may also be compelled to analyse the hazards posed by the ongoing dissemination and algorithmic amplification of harmful synthetic material.

iv. Strengthen protection for ordinary individuals

Celebrities should no longer be the primary focus of Indian personality-rights law. Regardless of their commercial or celebrity position, a person's right to regulate the unauthorized use of their identity and their right to reputation should be acknowledged. This is especially crucial as deepfake technology allows for widespread identity alteration.

v. Encourage cooperation between regulators, platforms and AI providers

Effective regulation cannot depend solely upon courts. AI developers, social-media platforms, regulators and law-enforcement authorities need clear responsibilities concerning detection, reporting, preservation of evidence and removal of harmful synthetic content. The European model demonstrates the value of distributing responsibility across the AI and digital ecosystem rather than placing the entire burden on the victim.

10.3 Conclusion:

The comparative study concludes that deepfakes pose a distinct and more complicated challenge to the right to reputation by allowing fraudulent representations of an individual's identity, conduct, and statements. Article 21, defamation, privacy and personality rights, and the intermediary responsibility, all give several paths of protection under Indian law. However, these remedies operate across multiple legal systems and are generally reactive, making effective and timely protection challenging, especially for persons lacking the wealth or public visibility of celebrities.

In contrast, the European Union has created a more structured regulatory framework by merging the GDPR, Digital Services Act, and Artificial Intelligence Act. While these instruments do not constitute a single legal right against reputational harm caused by deepfakes, they do address several aspects of the problem, such as personal data processing, platform responsibility, and transparency of AI-generated content. This tiered approach highlights the importance of combating deepfakes with both individual remedies and preventive regulatory

duties.

Therefore, the study concludes that India needs a more cohesive framework that links its current remedies with preventive protections rather than a whole new legal system. The current Indian system can be strengthened by mandatory and efficient labelling, provenance methods, more platform obligations, easily accessible takedown procedures, and more transparent protection of digital identity. By implementing these strategies, India will be able to offer more effective reputational protection against the quickly developing negative effects of deepfake technology, while also taking some cues from the European experience.