INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

DEEPFAKES, PERSONALITY RIGHTS AND PRIVACY IN INDIA: EXAMINING THE ADEQUACY OF THE EXISTING LEGAL FRAMEWORK

AUTHORED BY - PALAK GARG

ABSTRACT

The rapid development of generative artificial intelligence has transformed the manner in which digital content is created, manipulated and distributed. Among the most significant consequences of this technological transformation is the emergence of deepfakes, which are digitally generated or manipulated images, videos, audio recordings or other forms of media capable of realistically depicting a person as saying or doing something that the person never actually said or did. Although artificial intelligence-generated content may have legitimate applications in entertainment, education, accessibility, artistic expression and other fields, its misuse creates significant legal concerns relating to privacy, dignity, reputation, autonomy, identity and personality rights.

The problem is particularly significant in India because personality rights are not comprehensively codified in a single statute. Instead, protection is derived from constitutional principles, common law, intellectual property law, information technology legislation, criminal law and judicial decisions. The Supreme Court's recognition of privacy as a fundamental right in *Justice K.S. Puttaswamy (Retd.) v. Union of India* provides an important constitutional foundation for protecting individuals against unauthorized use and manipulation of personal identity. At the same time, Indian courts have increasingly recognized personality and publicity rights, particularly where a person's name, image, voice, likeness or other identifiable attributes are commercially exploited without authorization.

Recent judicial developments demonstrate the growing importance of this issue. In *Anil Kapoor v. Simply Life India*, the Delhi High Court specifically addressed unauthorized exploitation of an individual's name, image, likeness, voice and persona through technological tools including artificial intelligence, machine learning, deepfakes and face morphing. The Bombay High Court subsequently addressed AI-based voice cloning in *Arijit Singh v. Codible Ventures LLP*, recognizing that unauthorized AI tools capable of reproducing a celebrity's voice can implicate personality and publicity rights. These decisions demonstrate the ability of

ISSN: 2582-6433

existing legal principles to respond to emerging technological harms, but they also reveal limitations in the present framework.

India has recently moved toward more specific regulation of synthetically generated information. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 were amended on February 10, 2026 to introduce specific due-diligence obligations concerning synthetically generated information. The amended framework addresses certain unlawful synthetic content, including content that falsely depicts or portrays a natural person or real-world event in a manner likely to deceive, while also requiring prominent labelling and technical provenance mechanisms for certain other synthetic content. This development represents an important regulatory step, but questions remain concerning enforcement, victim remedies, intermediary responsibility, privacy, freedom of expression and the protection of personality rights.

This paper examines whether the existing Indian legal framework adequately protects individuals against deepfake-related violations of personality rights and privacy. It analyses the constitutional foundation of privacy, the judicial development of personality rights, the Information Technology Act, 2000, the Information Technology Rules, the Bharatiya Nyaya Sanhita, 2023, intermediary liability and recent regulatory developments. It further considers comparative approaches and identifies legal and practical gaps in the Indian framework. The paper argues that although existing constitutional, statutory and judicial mechanisms provide meaningful protection, the rapidly evolving nature of generative AI requires a more coherent framework that combines privacy protection, personality rights, intermediary accountability, technological transparency and effective remedies while preserving legitimate freedom of expression and technological innovation.

Keywords: Deepfakes, Artificial Intelligence, Personality Rights, Right to Privacy, Generative AI, Digital Identity, Intermediary Liability, Synthetic Media, Indian Law.

1. INTRODUCTION

Artificial intelligence has rapidly developed from a specialized technological field into a technology capable of influencing everyday social, commercial and legal interactions. Generative artificial intelligence systems can now create highly realistic photographs, videos, audio recordings and other forms of synthetic media. The increasing accessibility of such technologies has created significant opportunities for creativity and innovation, but it has simultaneously created new forms of legal harm. One of the most prominent manifestations of

ISSN: 2582-6433

this technological development is the deepfake.

The term "deepfake" generally describes digitally manipulated or synthetically generated content produced using artificial intelligence and machine-learning technologies. Deepfakes can alter a person's face, voice, expressions, gestures or other identifiable characteristics and can create realistic representations of events that never occurred. The technology is therefore capable of making fabricated content appear authentic. This creates an unusual legal problem because the harm may arise not from the unauthorized reproduction of an existing photograph or recording alone, but from the creation of an entirely new representation based upon characteristics associated with an identifiable individual.

The consequences of such manipulation can be serious. A person may be represented as making statements that they never made, participating in events in which they never participated, endorsing products that they never endorsed or appearing in situations that are inconsistent with their actual conduct. The resulting harm may involve reputation, dignity, privacy, professional interests and emotional well-being. Where the individual is a celebrity, the unauthorized use may additionally interfere with commercially valuable publicity and personality rights. However, the problem is not limited to celebrities. Ordinary individuals may also become victims of identity manipulation, impersonation, fraudulent communications and other forms of synthetic content.

The legal complexity arises because deepfakes can implicate several areas of law simultaneously. A particular deepfake may constitute an invasion of privacy, defamation, identity theft, cheating by personation, unauthorized commercial exploitation, copyright infringement or another form of unlawful conduct depending upon its content and purpose. Consequently, no single existing legal principle necessarily provides a complete solution to every deepfake-related dispute.

In India, this problem is particularly significant because personality rights have largely developed through judicial decisions rather than through a single comprehensive statutory framework. Courts have protected aspects of personality such as name, image, voice and likeness through principles derived from privacy, passing off, publicity rights and other legal doctrines. The constitutional recognition of privacy has further strengthened the legal foundation for protecting personal identity.

The Supreme Court's decision in *Justice K.S. Puttaswamy (Retd.) v. Union of India* established privacy as a constitutionally protected right. The judgment recognized privacy as connected with dignity, autonomy and liberty and placed it within the constitutional framework of Part III. The constitutional recognition of privacy is particularly relevant to deepfakes because

ISSN: 2582-6433

synthetic media may involve the unauthorized collection, processing, reproduction and manipulation of information associated with an individual's identity.

The judicial response to personality-right violations has also evolved significantly. In *Anil Kapoor v. Simply Life India*, the Delhi High Court considered a claim concerning unauthorized use of the actor's name, voice, image, likeness and other attributes of his persona. The Court expressly considered the misuse of artificial intelligence, machine learning, deepfakes and face morphing and granted protection against unauthorized exploitation.

The Bombay High Court's decision in *Arijit Singh v. Codible Ventures LLP* demonstrates a further development. The case concerned AI tools capable of generating content that replicated the singer's voice. The Court held at the interim stage that the plaintiff's name, voice, image, likeness and other personality traits were protectable and observed that making AI tools available for converting voices into that of a celebrity without permission constituted a violation of personality rights in the circumstances before the Court.

The regulatory landscape has also developed. On February 10, 2026, amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 introduced specific due-diligence provisions concerning synthetically generated information. The amended rules require certain technical measures to prevent unlawful synthetic information and address content that falsely depicts or portrays a natural person or real-world event in a manner likely to deceive. They also require specified synthetic information not falling within the prohibited categories to carry prominent labelling and, to the extent technically feasible, permanent metadata or other provenance mechanisms.

These developments raise the central question examined in this paper: whether the existing Indian legal framework adequately protects personality rights and privacy against the creation and dissemination of deepfakes. The paper examines this question through doctrinal analysis of constitutional provisions, statutes, subordinate legislation and judicial decisions. It also considers the tension between protection from harmful synthetic media and the constitutional protection of freedom of speech and expression.

2. UNDERSTANDING DEEPFAKES AND THE EMERGING LEGAL PROBLEM

Deepfakes represent a significant development in digital manipulation because they permit the creation of synthetic content that can closely resemble authentic photographs, recordings or videos. Traditional image and video manipulation has existed for decades, but advances in

ISSN: 2582-6433

machine learning have substantially increased the sophistication, accessibility and scalability of synthetic media. A user may potentially create content involving another person's face or voice without requiring access to professional production facilities.

The legal significance of deepfakes arises primarily from the ability of such content to interfere with identity. Identity is not limited to a person's legal name. An individual's face, voice, mannerisms, appearance, signature and other recognizable characteristics may become associated with that person to such an extent that their unauthorized replication can create a false impression of participation or endorsement.

Deepfakes therefore challenge traditional legal assumptions concerning representation. A conventional infringement may involve copying an existing work or recording. A deepfake may instead involve training or manipulating an artificial intelligence system to produce new content that resembles a particular person. This distinction becomes important when determining which legal rights have been violated.

The potential uses of synthetic media are not inherently unlawful. Artificial intelligence can facilitate dubbing, accessibility, educational material, historical reconstruction, film production, entertainment and creative experimentation. Regulation must therefore avoid treating all synthetic media as inherently harmful. The legal question should instead focus upon the nature of the representation, the consent of the person concerned, the purpose of the content, the likelihood of deception and the rights or interests affected.

The risk becomes considerably greater where the synthetic content falsely portrays a natural person as engaging in conduct or making statements that never occurred. The February 2026 amendment to the IT Rules recognizes this concern by specifically addressing synthetically generated information that falsely depicts or portrays a natural person or real-world event in a manner likely to deceive.

The problem is further complicated by the speed of online dissemination. Once synthetic content is uploaded, it may be copied, reposted and modified by numerous users across multiple platforms. A person seeking removal may therefore face a situation in which the original content is removed but substantially similar copies continue to circulate.

The transnational nature of the internet adds another difficulty. A person in India may become the subject of a deepfake created in another country, uploaded through a foreign platform and accessed by users throughout the world. Determining jurisdiction and securing effective enforcement may consequently be difficult. These characteristics demonstrate why deepfake regulation cannot be considered exclusively as a question of criminal liability. It also requires attention to privacy, civil remedies, intermediary responsibility, technological standards and

ISSN: 2582-6433

international cooperation.

3. PERSONALITY RIGHTS IN INDIA: CONCEPT, SCOPE AND JUDICIAL DEVELOPMENT

Personality rights broadly refer to legal interests associated with the identity and recognizable attributes of an individual. Such attributes may include name, image, likeness, voice, signature, appearance, mannerisms and other characteristics through which a person can be identified. Personality rights are closely associated with the concept of publicity rights, particularly where the identity of an individual possesses commercial value.

Indian law does not contain a single comprehensive legislation expressly defining and regulating personality rights. Instead, courts have developed the doctrine through a combination of privacy principles, intellectual property concepts, passing off, unfair competition and other common-law principles. This judicial development has been particularly important in cases involving celebrities because their identities may possess substantial commercial value.

The distinction between privacy rights and publicity rights is important. Privacy primarily concerns an individual's interest in controlling personal information, identity and private life, whereas publicity rights concern the commercial exploitation of identity. The two rights may overlap, particularly where unauthorized commercial use of a person's identity also affects dignity or autonomy.

The Supreme Court's decision in *R. Rajagopal v. State of Tamil Nadu* provides an important foundation for the relationship between privacy and unauthorized use of personal identity. The decision recognized privacy as including a right to be left alone and discussed the unauthorized publication of aspects of an individual's life and identity. The principles discussed in *Rajagopal* have subsequently been considered by courts dealing with personality-related claims.

The Delhi High Court's decision in *Anil Kapoor v. Simply Life India* is particularly significant for the modern deepfake context. The plaintiff sought protection over his name, voice, photograph, image, likeness, mannerisms and other elements of his personality. The Court considered various forms of unauthorized use, including morphed images, commercial merchandise and technologically manipulated representations.

The Court recognized that technological developments have made it possible for unauthorized users to reproduce or imitate a celebrity's persona through artificial intelligence and other tools.

ISSN: 2582-6433

It specifically referred to AI, machine learning, deepfakes and face morphing and held that the plaintiff's name, likeness, image and persona deserved protection against the unauthorized uses established in the case.

The importance of *Anil Kapoor* lies not merely in the relief granted to one celebrity but in the manner in which the Court connected technological manipulation with existing legal protections. Rather than treating deepfakes as an entirely new category requiring an entirely new cause of action, the Court applied established principles relating to personality rights, privacy and unlawful commercial exploitation to technologically novel conduct.

The Bombay High Court's decision in *Arijit Singh v. Codible Ventures LLP* further illustrates this development. The plaintiff complained of AI platforms and other services capable of generating artificial versions of his voice. The Court considered the plaintiff's name, voice, manner of singing, image, likeness, signature and persona as protectable attributes. It also considered the commercial implications of AI-generated voice content.

Significantly, the Court observed that making AI tools available to convert a voice into that of a celebrity without permission constituted a violation of personality rights in the circumstances before it. The Court also recognized that AI-generated content could potentially affect the career and livelihood of a performer by enabling third parties to appropriate characteristics that are central to the performer's professional identity.

These decisions indicate that Indian courts are increasingly prepared to recognize voice as an important element of personality. This is particularly important in the age of generative AI because voice cloning can be used to create highly convincing audio representations without requiring a traditional recording by the person concerned.

The judicial development of personality rights nevertheless has limitations. Because the doctrine has developed through case law rather than comprehensive legislation, its precise scope may depend upon the facts of each case. Questions concerning whether personality rights extend to ordinary individuals, how long such rights survive, whether they are inheritable, and how they should be balanced against freedom of expression remain areas requiring further clarification.

4. DEEPFAKES AND THE CONSTITUTIONAL RIGHT TO PRIVACY

The constitutional right to privacy provides an essential foundation for understanding the legal implications of deepfakes. Article 21 of the Constitution protects life and personal liberty, and judicial interpretation has expanded the meaning of these guarantees to encompass dignity, autonomy and other aspects of individual freedom.

ISSN: 2582-6433

The Supreme Court's decision in *Justice K.S. Puttaswamy (Retd.) v. Union of India* represents the most significant constitutional development concerning privacy in India. The Court recognized privacy as a fundamental right and emphasized its relationship with liberty, dignity and autonomy. The judgment also recognized informational privacy as an important component of the broader right to privacy.

The recognition of informational privacy is particularly significant in the context of deepfakes. Artificial intelligence systems may rely upon photographs, videos, audio recordings and other publicly or privately available information to generate synthetic representations. The fact that a particular photograph or recording is publicly accessible does not necessarily mean that every subsequent use of the information is legally permissible.

Deepfakes may interfere with informational privacy because an individual may lose control over how information associated with their identity is used. A photograph uploaded for an ordinary purpose may subsequently be processed to create a synthetic video representing the individual in an entirely different situation. Similarly, an audio recording may be used to construct artificial speech that the person never produced.

Privacy also has an autonomy dimension. A person's ability to control how their identity is represented is closely related to individual autonomy. A deepfake that falsely depicts an individual as making statements or engaging in conduct can interfere with that person's ability to determine how they are represented to others.

The dignity dimension is equally important. The constitutional conception of dignity recognizes the individual as an autonomous person rather than merely an object of technological or commercial manipulation. Deepfakes that humiliate, degrade or falsely associate an individual with objectionable conduct may therefore raise concerns extending beyond economic injury.

The relationship between privacy and personality rights can be seen clearly in *Anil Kapoor*. The Delhi High Court expressly connected unauthorized exploitation of the plaintiff's persona with privacy and dignity. The Court observed that technological tools now make it possible for unauthorized users to use or imitate a celebrity's persona through artificial intelligence and deepfakes and emphasized that the Court could not ignore such misuse.

At the same time, privacy is not an unlimited right. The constitutional framework requires a balance between privacy and competing interests, including freedom of expression. The Supreme Court's privacy jurisprudence recognizes that restrictions on privacy must satisfy constitutional requirements concerning legality, legitimate state purpose and proportionality. This becomes particularly important when regulation of synthetic media affects satire, parody,

ISSN: 2582-6433

artistic expression or legitimate criticism.

5. THE INDIAN LEGAL FRAMEWORK GOVERNING DEEPFAKES

The Indian legal framework governing deepfakes is composed of several layers of law. The Information Technology Act, 2000 provides important statutory mechanisms for addressing digital misconduct. Depending upon the circumstances, provisions concerning identity theft, cheating by personation, privacy violations and sexually explicit material may become relevant to synthetic content.

Section 66C of the Information Technology Act concerns identity theft, while Section 66D addresses cheating by personation using a computer resource or communication device. Section 66E addresses violation of privacy. These provisions may apply to certain forms of deepfake conduct where the required statutory elements are satisfied.

The challenge is that these provisions were not originally enacted as a comprehensive deepfake regulatory regime. Consequently, their application depends upon the particular facts and legal characterization of the conduct. A deepfake that merely reproduces a celebrity's appearance for commercial advertising may raise different legal questions from a deepfake used to commit fraud or a deepfake that falsely portrays an individual in unlawful or degrading conduct.

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 provide another important layer of protection. Intermediaries are subject to due-diligence obligations and mechanisms for addressing unlawful or harmful content. The framework becomes particularly relevant because social-media and content-sharing platforms can facilitate the rapid dissemination of deepfakes.

The most significant recent development is the February 10, 2026 amendment concerning synthetically generated information. The amendment introduces a specific due-diligence provision for intermediaries whose services may enable the creation, generation, modification, publication, transmission, sharing or dissemination of synthetically generated information. The provision requires reasonable and appropriate technical measures to prevent specified unlawful synthetic content.

The amendment specifically identifies certain categories of unlawful synthetic information, including content that is obscene, pornographic, invasive of privacy, or constitutes non-consensual intimate imagery. It also addresses false documents and electronic records and, importantly for the present research, synthetic content that falsely depicts or portrays a natural person or real-world event by misrepresenting identity, voice, conduct, action or statement in a manner likely to deceive.

ISSN: 2582-6433

The amended rules also introduce transparency requirements. Synthetic information falling outside the specified prohibited categories must, subject to the rule's requirements, be prominently labelled so that it can be identified as synthetically generated. The provision further contemplates permanent metadata or other technical provenance mechanisms, to the extent technically feasible, including a unique identifier capable of identifying the computer resource used for creation or alteration.

This development is significant because it moves Indian intermediary regulation beyond a general reliance on existing cyber offences. It recognizes synthetic media as a distinct technological phenomenon requiring specific due diligence.

The Bharatiya Nyaya Sanhita, 2023 may also apply to certain forms of deepfake conduct. Although the BNS does not constitute a dedicated deepfake statute, conduct involving cheating, impersonation, defamation, intimidation or other offences may fall within the relevant provisions depending upon the facts. The criminal-law response is therefore potentially available where synthetic media is used as a means of committing a recognized offence.

Intellectual property law may also become relevant. The Copyright Act, 1957 may apply where protected works are copied or manipulated without authorization. In the context of AI-generated voice or image content, however, copyright may not always provide a complete remedy because the harm may concern the individual's identity rather than the copying of a particular copyrighted work.

The Digital Personal Data Protection Act, 2023 is relevant to the broader question of processing personal data in the digital environment. Its principles may become increasingly important as AI systems process personal information for the development and operation of generative systems. Nevertheless, the relationship between data protection law and personality rights requires careful analysis because not every personality-related harm can be reduced to a question of personal-data processing.

6. INTERMEDIARY LIABILITY AND PLATFORM RESPONSIBILITY

Intermediaries occupy a central position in the deepfake ecosystem because they can facilitate both the creation and dissemination of synthetic content. Social-media platforms, video-sharing services, cloud storage providers and AI platforms may each perform different functions in relation to synthetic media.

Section 79 of the Information Technology Act provides a safe-harbour framework for intermediaries subject to specified statutory conditions. The framework reflects an attempt to balance platform liability with the practical reality that intermediaries may host enormous

ISSN: 2582-6433

quantities of user-generated content.

The challenge becomes more complex when the platform itself provides tools capable of generating synthetic content. A platform that merely hosts an uploaded deepfake may occupy a different legal position from a platform that actively provides an AI model or feature enabling users to create a convincing replica of another person's voice or appearance.

The *Arijit Singh* litigation illustrates this distinction. The case involved AI platforms capable of converting voices into an artificial version of the plaintiff's voice. The Bombay High Court considered not only the content generated by users but also the availability and promotion of technological tools that enabled unauthorized replication.

The February 2026 IT Rules attempt to address this technological dimension by imposing specific obligations on intermediaries whose computer resources may enable, permit or facilitate the creation or dissemination of synthetically generated information. This reflects an important shift from regulating only the uploader toward considering the technological architecture through which synthetic media is created and distributed.

Nevertheless, platform regulation raises concerns about over-removal. If platforms are given broad obligations to detect and remove synthetic content, they may become incentivized to remove lawful parody, satire, artistic expression or political commentary merely because it has been manipulated. The legal framework must therefore distinguish unlawful deceptive content from legitimate expression.

The requirement of technical provenance may help address this difficulty by improving transparency rather than requiring the removal of all synthetic media. Labelling can enable users to understand whether content is AI-generated while allowing lawful content to remain accessible.

However, labelling alone may not prevent harm. A clearly labelled deepfake may still damage reputation, violate privacy or exploit a person's identity. Therefore, provenance mechanisms should complement rather than replace substantive legal remedies.

7. JUDICIAL RESPONSE TO AI-GENERATED PERSONALITY RIGHTS VIOLATIONS

Indian courts have increasingly responded to technological changes through the development of existing legal doctrines. The decisions concerning Anil Kapoor and Arijit Singh are particularly significant because they demonstrate how personality rights can be applied to artificial intelligence and synthetic media.

ISSN: 2582-6433

In *Anil Kapoor v. Simply Life India*, the Delhi High Court considered various unauthorized uses of the actor's identity, including morphed images, merchandise, voice recordings and other representations. The Court recognized that technological tools could be used to reproduce or imitate the plaintiff's persona and specifically referred to artificial intelligence, machine learning, deepfakes and face morphing.

The Court emphasized that fame does not eliminate legal protection. Although public figures may be subject to legitimate criticism, satire and public discussion, the unauthorized exploitation of their identity for commercial purposes may cross the boundary between protected expression and unlawful conduct. The Court therefore granted protection against the uses established in the case.

The decision is particularly important because it recognizes the interconnected nature of personality, privacy and commercial interests. The Court did not treat the plaintiff's image merely as an intellectual property asset. It also considered the impact of misuse upon dignity, privacy and livelihood.

The *Arijit Singh* decision builds upon this approach by recognizing the significance of voice as a personality attribute. The Bombay High Court considered allegations that AI tools were being used to convert speech and other audio recordings into an artificial version of Singh's voice.

The Court found that the plaintiff's name, voice, image, likeness, mannerisms and persona were protectable aspects of his personality rights. It further held at the interim stage that making AI tools available to convert a voice into that of a celebrity without permission constituted a violation of personality rights.

The decision also demonstrates the importance of commercial exploitation in personality-right litigation. The Court observed that unauthorized AI-generated content could potentially affect a performer's career and livelihood by allowing third parties to exploit the attributes that make the performer commercially identifiable.

The judicial approach, however, should not be interpreted as establishing that every AI-generated reference to a public figure is unlawful. The courts have repeatedly recognized the importance of freedom of speech, criticism, parody and other legitimate forms of expression. The precise boundary will depend upon factors including identifiability, consent, commercial purpose, deception, harm and the nature of the use.

8. DEEPFAKES AND FREEDOM OF SPEECH AND EXPRESSION

Article 19(1)(a) of the Constitution protects freedom of speech and expression. This constitutional guarantee is directly relevant to deepfake regulation because synthetic content

ISSN: 2582-6433

can serve legitimate expressive purposes.

Satire and parody may involve deliberate alteration of a person's appearance or voice. Political commentary may also use manipulated or fictionalized representations. Artistic works may employ synthetic media to create characters or narratives. A regulatory system that automatically prohibits all manipulated content would risk interfering with legitimate expression.

The Delhi High Court's discussion in *Anil Kapoor* recognizes this tension. The Court acknowledged that free speech concerning well-known persons includes information, news, satire, parody and genuine criticism. The problem arises when such expression crosses into unauthorized exploitation or tarnishment of personality.

The same principle appears in *Arijit Singh*, where the Bombay High Court recognized that freedom of speech permits critique and commentary but does not necessarily provide a licence for commercial exploitation of a celebrity's persona.

The legal framework should therefore focus on the characteristics of the harmful conduct rather than merely the fact that artificial intelligence has been used. A deepfake created for an obvious parody and clearly presented as fictional may require different treatment from a deepfake falsely portraying an individual as making a real statement or endorsing a commercial product.

The 2026 IT Rules attempt to address deception by focusing upon synthetic information that falsely depicts or portrays a natural person or real-world event in a manner likely to deceive. This approach is significant because it recognizes that deception, rather than synthetic creation alone, may be a key factor in determining regulatory concern.

Nevertheless, the concept of deception may itself raise interpretive questions. What is "likely to deceive" may vary depending upon context, audience and presentation. A sophisticated viewer may immediately recognize a parody, whereas another viewer may believe the representation to be authentic. Courts and regulators will therefore need to interpret the provision carefully.

A balanced approach should protect individuals against harmful impersonation and deceptive exploitation while preserving legitimate criticism and creative expression. The objective should not be to eliminate synthetic media but to prevent unlawful uses that cause legally recognizable harm.

9. COMPARATIVE LEGAL PERSPECTIVE

The development of deepfake regulation is not unique to India. Other jurisdictions have also struggled to balance innovation, freedom of expression, privacy and protection from synthetic

ISSN: 2582-6433

deception.

The European Union has adopted a broader regulatory approach to artificial intelligence through the EU Artificial Intelligence Act. The European approach includes transparency obligations for certain AI-generated and manipulated content and reflects an effort to regulate artificial intelligence according to risk. The EU model demonstrates the possibility of addressing synthetic media within a broader AI governance framework rather than relying exclusively upon traditional criminal or civil law.

The European approach is relevant to India because it emphasizes transparency and accountability. However, the European constitutional and regulatory environment differs from India, and the EU framework cannot simply be transplanted into Indian law. India must consider its own constitutional protections, technological environment and institutional capacities.

The United States presents a more fragmented regulatory landscape. Different forms of deepfake harm may be addressed through state laws, privacy principles, publicity rights, defamation law, intellectual property law and other existing legal mechanisms. The American approach illustrates the importance of protecting freedom of expression, particularly where synthetic content is used for political commentary or artistic purposes.

The United Kingdom has also developed legal responses to harmful digitally manipulated content, particularly in relation to intimate imagery and online safety. Its regulatory developments demonstrate the growing international recognition that existing legal categories may need adaptation to address AI-generated harms.

Comparative experience suggests that no single regulatory model provides a complete answer. Effective regulation is likely to require a combination of transparency, platform accountability, individual remedies and substantive restrictions on particularly harmful forms of synthetic media.

For India, the comparative lesson is that deepfake regulation should not be approached solely through criminalization. A comprehensive framework should also facilitate rapid civil remedies, platform accountability, technological provenance and effective mechanisms through which victims can regain control over their identity.

10. LEGAL GAPS AND CHALLENGES IN THE INDIAN FRAMEWORK

Despite the significant development of Indian law, several gaps remain. The first concern is the absence of a comprehensive statutory framework specifically consolidating personality rights and deepfake-related harms. Although the 2026 amendment to the IT Rules provides a

ISSN: 2582-6433

more specific regulatory mechanism for synthetic information, personality rights continue to be substantially dependent upon judicial development.

This may create uncertainty concerning the precise scope of the right. Questions concerning the protection of ordinary individuals, posthumous personality rights, inheritance, licensing, consent and exceptions for legitimate expression may require further statutory clarification.

A second challenge concerns identification of creators. Deepfake creators may operate anonymously or use foreign platforms. Even where the harmful content is detected, identifying the person responsible may require cooperation between platforms, service providers and law-enforcement authorities.

A third problem is the speed of dissemination. A conventional lawsuit may take time, whereas harmful synthetic content can become widely distributed within hours. Effective regulation therefore requires procedures capable of providing rapid interim relief.

A fourth challenge concerns cross-border enforcement. A deepfake affecting an Indian resident may be created outside India and hosted on a platform incorporated in another jurisdiction. Questions concerning jurisdiction, applicable law and enforcement of judicial orders can become difficult.

A fifth concern is technological detection. Deepfake detection tools themselves are developing alongside generative systems. As synthetic media becomes increasingly sophisticated, reliance solely upon visual or auditory detection may become inadequate. Technical provenance, watermarking, metadata and content credentials may therefore become increasingly important.

A sixth challenge concerns the relationship between personality rights and freedom of expression. A legal framework that grants excessively broad control over one's likeness could potentially suppress legitimate commentary, parody and artistic expression. The law must therefore distinguish between unauthorized commercial exploitation, deceptive impersonation and legitimate expressive use.

A seventh concern relates to remedies. Victims may require more than monetary compensation. They may need urgent removal, correction, disclosure of the source, preservation of evidence, prevention of further dissemination and protection against repeated uploads. A meaningful legal framework should therefore provide remedies suited to the nature of digital harm.

11. RECOMMENDATIONS AND THE WAY FORWARD

India's developing framework provides a foundation for addressing deepfakes, but further clarification would improve legal certainty. One possible approach would be to establish a consolidated statutory framework dealing with synthetic media and personality-related harms.

ISSN: 2582-6433

Such legislation could define deepfakes in technology-neutral language and establish clear distinctions between lawful synthetic expression and unlawful deceptive or exploitative content.

The law should recognize that personality is multidimensional. Protection should not be limited to photographs or names but should extend, where legally justified, to voice, likeness, mannerisms, distinctive characteristics and other attributes capable of identifying an individual.

Consent should form an important component of the regulatory framework. Where a person's identity is reproduced or manipulated for commercial or deceptive purposes, the absence of authorization should be an important factor. At the same time, consent requirements should not unnecessarily interfere with legitimate criticism, news reporting, parody or artistic expression.

A rapid redress mechanism should also be developed. Individuals affected by unlawful deepfakes should be able to submit complaints through accessible procedures and seek prompt removal or restriction of access. This mechanism should coexist with judicial remedies for cases involving significant or contested harm.

Intermediaries should maintain transparent processes for responding to complaints and should be required to preserve relevant evidence where necessary for legal proceedings. However, platform obligations should be sufficiently precise to avoid incentivizing excessive removal of lawful content.

The use of provenance technology should also be encouraged. The February 2026 amendments already contemplate permanent metadata or other appropriate technical provenance mechanisms to the extent technically feasible. The development of interoperable provenance standards could help users identify the origin and synthetic nature of digital content.

Legal regulation should also recognize differences between AI developers, AI service providers, social-media platforms, content hosts and individual users. Liability should not automatically be imposed upon every actor connected to synthetic content. Instead, responsibility should depend upon the actor's role, knowledge, control, conduct and compliance with applicable obligations.

The development of judicial guidelines would further assist courts. Courts increasingly encounter applications involving AI-generated content, and consistent principles concerning identifiability, commercial use, consent, deception, privacy and freedom of expression could improve predictability.

Finally, public awareness is essential. Legal remedies cannot completely eliminate the social effects of deepfakes. Users need to understand that apparently authentic photographs, videos and voices may be artificially generated. Digital literacy and technological awareness should

ISSN: 2582-6433

therefore accompany legal regulation.

12. CONCLUSION

Deepfakes represent a significant challenge to contemporary legal systems because they undermine traditional assumptions concerning the authenticity of visual and auditory information. The ability to reproduce a person's face, voice, likeness or mannerisms through artificial intelligence can interfere with privacy, dignity, reputation, autonomy and personality rights. The problem is particularly serious when synthetic content is designed to deceive viewers or commercially exploit an individual's identity without consent.

Indian law has already developed several mechanisms capable of addressing different aspects of this problem. Constitutional privacy jurisprudence provides a strong foundation for protecting personal autonomy and dignity. The Information Technology Act, 2000 addresses various forms of digital misconduct, while the IT Rules impose intermediary due-diligence obligations. Criminal law, intellectual property law and civil remedies may also become relevant depending upon the circumstances.

Judicial decisions have played a particularly important role. *Anil Kapoor v. Simply Life India* demonstrates that Indian courts are willing to extend personality-right protection to technologically advanced forms of unauthorized exploitation, including artificial intelligence, machine learning, deepfakes and face morphing. *Arijit Singh v. Codible Ventures LLP*further demonstrates that AI-based voice cloning can implicate personality rights where a person's distinctive voice is replicated and commercially exploited without authorization.

The February 2026 amendment to the IT Rules represents an important development because it specifically regulates synthetically generated information and addresses deceptive synthetic representations of natural persons and real-world events. It also introduces labelling and technical provenance requirements for specified synthetic content. This indicates that Indian regulation is moving toward a more technologically specific approach.

Nevertheless, the existing framework remains fragmented. Personality rights continue to depend substantially upon judicial development, while victims may face difficulties relating to identification of perpetrators, rapid dissemination, cross-border enforcement, technological detection and access to effective remedies. The coexistence of legitimate synthetic expression and harmful manipulation further complicates regulation.

The appropriate response is therefore unlikely to be an absolute prohibition on deepfake technology. Instead, Indian law should seek to regulate harmful uses while preserving technological innovation and constitutionally protected expression. A coherent framework

ISSN: 2582-6433

should combine privacy protection, personality rights, intermediary accountability, transparency, provenance mechanisms and rapid victim remedies.

The central legal objective should be to ensure that technological innovation does not eliminate individual control over identity. A person's face, voice and recognizable identity are increasingly capable of being reproduced by machines, but the legal system must ensure that technological capacity does not automatically become legal permission. The future development of Indian law should therefore focus on maintaining a balance between innovation and individual rights, ensuring that the benefits of artificial intelligence are not achieved at the cost of privacy, dignity, autonomy and personality.

REFERENCES

Primary Legal Sources

Constitution of India, 1950.

Information Technology Act, 2000.

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended.

Bharatiya Nyaya Sanhita, 2023.

Digital Personal Data Protection Act, 2023.

Copyright Act, 1957.

Trade Marks Act, 1999.

Cases

Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

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

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

Arijit Singh v. Codible Ventures LLP & Ors., Bombay High Court, Interim Application (L) No. 23560 of 2024, order dated July 26, 2024.

D.M. Entertainment Pvt. Ltd. v. Baby Gift House, 2010 SCC OnLine Del 4790.

Titan Industries Ltd. v. Ramkumar Jewellers, 2012 SCC OnLine Del 2382.

Shivaji Rao Gaikwad v. Varsha Productions, 2015 SCC OnLine Mad 158.

Government and Regulatory Materials

Ministry of Electronics and Information Technology, Government of India, Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended

ISSN: 2582-6433

by G.S.R. 120(E), dated February 10, 2026.

Ministry of Electronics and Information Technology, Government of India, Draft Amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 relating to synthetically generated information, October 22, 2025.