A STUDY ON DEEPFAKES IN THE CONTEXT OF DIGITAL PROPERTY IN INDIA

Sanjana. A, St. Joseph's College of Law

I. ABSTRACT

The exponential advancement of deepfake technology has enabled the generation of hyper-realistic synthetic media, severely blurring the boundary between authentic and fabricated content. This technological evolution challenges established legal paradigms regarding consent, proprietary interests in digital likeness, and bodily privacy. When someone's photo is taken from social media and turned into a deepfake without consent, what exactly has been violated? Is it just a misused picture, or something deeper involving property, privacy, and identity? Can a photograph even be called "Property" under Indian law? This paper looks at India's current laws, The Information Technology Act, the Bharatiya Nyaya Sanhita, and the Copyright Act along with privacy and personality rights, to ask who is really responsible when a deepfake causes harm, and whether victims today have any real way to fight back.

Keywords: Deepfakes, Intellectual Property, Artificial Intelligence, Information Technology, Personality Rights.

II. INTRODUCTION:

The rapid growth of artificial intelligence has completely changed how we make, share and view digital content. One of the biggest breakthroughs in this area is deepfake technology, which allows people to create incredibly realistic but completely fake pictures, videos, and voice recordings. By using advanced computer systems, specifically deep learning software. Deepfake can copy a person's face, voice and unique habits almost perfectly.[1]

Even though deepfakes have good uses in areas like movies, school lessons, advertising and creative arts, using them maliciously has caused major legal, moral, and social problems. People have used deepfakes to spread fake news, trick voters, steal identities, cheat people out of money, and create explicit content without the victims permission.[2] Doing this hurts people by invading their privacy, damaging their dignity, and ruining their reputations, while also destroying the public's trust in online media and democratic systems.[3]

In India, the growing accessibility of artificial intelligence tools and the widespread use of social media platforms have intensified the risks associated with deepfake technology. Several incidents involving manipulated videos of public figures, celebrities, and private individuals have highlighted the vulnerability of citizens in the digital environment.[4] The ability of deepfakes to create convincing yet false representations raises important questions regarding consent, ownership of digital identity, privacy rights, and legal accountability.

The emergence of deepfakes presents a unique challenge to the existing legal framework. While provisions under the Act of Information Technology, 2000 and the 2023 Criminal Legislation provide certain remedies, they were not specifically designed to address AI-generated synthetic media.[5] Because of this, problems like using someone's pictures without permission, violating personal identity rights, online crimes, and proving whether digital evidence is real are still not being handled well enough. This paper looks at how deepfake technology affects the unauthorised use of online photos and the legal rights connected to them

[1] Bhale, Swanand, Deepfake Laws in India: The Need for Legal Regulation in the AI Era (February 01, 2025) . Available at SSRN:http://dx.doi.org/10.2139/ssrn.5153296 > accessed 3 June 2026
[2] R, Sarferaaz Khaan, Countering Deepfakes: A Strategic Blueprint for Modernizing Indian Criminal Law (November 27,2025). International Journal for Legal Research and Analysis, Volume 2, Pp. 6-7, Available at SSRN:http://dx.doi.org/10.2139/ssrn.591854> accessed 3 June 2026
[3] ADABALA, DIMPLE SAHITHI, When Technology Lies: Deepfake and Criminal Law in India (April 28, 2026). Available at SSRN:http://dx.doi.org/10.2139/ssrn.6665081 > accessed 3 June 2026
[4] Thakur, Dushyant Singh, Deepfakes as Human Rights Violations: Rethinking Dignity and Privacy in India (September 10, 2025). Available at SSRN:http://dx.doi.org/10.2139/ssrn.5532383 > accessed 3 June 2026

in India. It examines the threats deepfakes pose to a person's privacy, identity, reputation, and property, while checking how well current laws actually work to fix these issues. Finally, the study explores why India needs a complete and updated set of laws, that can protect individual rights in the digital age without stopping technological progress.[6]

III. RESEARCH OBJECTIVES

1. To examine whether personal images shared on social media can be classified as "property" under the Transfer of Property Act, 1882.

2. To analyse whether the creation and circulation of deepfake content using an individual's image violates intellectual property rights, privacy rights and personality rights under Indian law.

3. To determine the liability of deepfake creators and social media intermediaries under the existing Indian legal framework.

4. To evaluate the adequacy of the legal remedies currently available to victims of deepfake misuse in addressing emerging digital harms.

5. To suggest legal and policy reforms necessary for effectively regulating deepfake misuse and protecting individual digital rights in India.

IV. RESEARCH METHODOLOGY

This study adopts a doctrinal and qualitative research methodology based on secondary sources. Data has been collected from statutes, judicial decisions, government advisories, international instruments, journal articles, books and online reports. The study analyses the existing Indian legal framework governing deepfakes and undertakes a limited comparative analysis with international regulatory models such as the European Union AI Act and the United Kingdom Online Safety Act.

[5] Farish,Kelsey,Do Deepfakes Pose a Golden Opportunity Considering Whether English Law Should Adopt California's Publicity Right in the Age of the Deepfake (September 1, 2019). Available at SSRN:http://dx.doi.org/10.2139/ssrn.3648960 >accessed 3 June 2026

[6] Priyanshu Yadav,Stolen Faces,Borrowed Voices:The Legal Imperative for Regulating Deepfake in India,DOI: https://doij.org/10.10000/IJLMH.1111413> accessed 3 June 2026

V. DEEPFAKE TECHNOLOGY

UNDERSTANDING DEEPFAKE TECHNOLOGY

5.1 HISTORY AND ORIGIN

Deepfake technology originated in 1997 with the development of Video Rewrite, a software that could alter video footage to make individuals appear to say words they never spoke. Initially, such technologies were created for legitimate purposes like film editing and visual effects. The introduction of Generative Adversarial Networks (GANs) in 2014 significantly improved the realism of synthetic media. As deepfake tools became more accessible, their use expanded beyond research and entertainment to include non-consensual pornography, misinformation, political manipulation, and online fraud. Consequently, deepfakes have evolved into a major social, ethical, and legal challenge.

5.2 HOW DEEPFAKES WORK

Generative Adversarial Networks (GANs), introduced in 2014, are a type of artificial intelligence system consisting of two competing neural networks: a Generator and a Discriminator. The Generator creates synthetic content, while the Discriminator evaluates whether the content is real or artificially generated. Through a continuous process of adversarial optimization, both neural networks iteratively enhance their respective algorithmic accuracy. This iterative feedback loop enables GANs to synthesize High-fidelity visual and auditory content which is exactly how modern deepfakes are made.[7]

5.3 TYPES OF DEEPFAKES

Deepfakes come in several different types, including fake videos, audio recordings, and written texts. Each type uses artificial intelligence in its own way to copy mimic how a real person looks, speaks, moves or writes. Understanding these categories is important because it helps in recognising how deepfake technology can be created and potentially misused in various contexts. Deepfakes can broadly be classified into Five types:

1. Face-Swapped Videos: This type involves replacing one person's face with another in a video while keeping the original body and movements. AI ensures that facial expressions and movements remain consistent and realistic across frames.

Example: A video showing a celebrity appearing in a movie scene they never actually acted in.

2. Lip-Syncing and Audio-Visual Manipulation: In this form, a video is altered so that the mouth movements match a different or artificially generated audio track. When combined with voice cloning, it creates a highly convincing illusion of speech.

Example: A leader appearing to give a statement in a video where both the voice and lip movements have been digitally altered.

In March 2022, a deepfake video of Ukrainian President Volodymyr Zelenskyy was circulated online, in which he appeared to urge Ukrainian soldiers to surrender during the ongoing Russia-Ukrainians war. The fabricated video was shared through hacked media platforms and social media channels in Ukraine, but it was quickly identified as false and debunked by authorities.[8]

3. Voice Cloning(Audio Deepfakes): This type focuses on reproducing a person's voice using AI without any visual element. The system learns speech patterns, tone, and rhythm to generate realistic audio.

Example: A fake phone call where someone copies a bank manager's voice and asks the victim to share their account details.

4. Full-Body Reenactment: This AI technology copies one person's exact movement, gestures, and poses and places them onto a different person. This technology synthesizes behavioural patterns and spatial dynamics, transposing an individual's behavioural likeness onto a distinct background context.

Example:A video that shows someone doing a dance or a sports routine that they never actually performed in real life.

5. Text-Based Conversational Clones: Natural Language Processing (NLP) models simulate an individual's linguistic style, syntax and textual idiosyncrasies to orchestrate sophisticated social engineering and financial fraud.

Example: A text that looks exactly like it's from a friend, copying the way they usually talk, to

[7] Daniel Miller,Klaire Somoray and Hallev Stevens, A Shallow History of Deepfakes Pp.2-16. Available at SSRN:https://dx.doi.org/10.2139/ssrn.5130379>accessed 4 June 2026

trick you into sending them money quickly.[9]

5.4 DEEPFAKES ON SOCIAL MEDIA

Social media intermediaries act as primary vectors for the viral dissemination of synthetic media. Their proprietary recommendation algorithms are engineered to optimize user engagement, frequently prioritising sensationalist or polarizing content.

Social media platforms are a big reason why deepfakes spread so fast. Their systems are designed to push exciting or shocking videos because those get the most views and comments, meaning a fake video can go before anyone realizes it is a fake.

It is also incredibly easy for users to quickly copy and share these videos across apply like Facebook, TikTok, Instagram, and WhatsApp. Once a deepfake is out there, it is almost impossible to delete completely or track down who originally made it.[10,11]

5.5 REAL WORLD HARMS

Deepfakes are dangerous in real life because they can spread lies, ruin reputations, and make people lose trust in what they see online. When they are misused, they can harm regular people, governments, and the economy.

---

[8]BBC News,'Deepfake of Zelensky circulating online'(BBC News, 17 March 2022) https://www.bbc.com/news/technology-60780142 >accessed 6 June, 2026

[9] SentinelOne, 'Deepfakes: Definition, Types, and Key Examples(16 July2025)https://www.sentinelone.com/cybersecurity-101/cybersecurity/deepfakes/>accessed 6 June 2025

[10] CyberPeace Foundation, 'The Efforts of Social Media Platforms to Counter Deepfake(CyberPeace,n.d.)https://www.cyberpeace.org/resources/blogs/the-efforts-of-social-media-platforms-to-counter-deepfake >accessed 6 June 2026

[11] NBC News, 'Deepfake scams have arrived on Facebook, TikTok and YouTube' (NBC News,n.d.)https://www.nbcnews.com/tech/tech-news/deepfake-scams-arrived-fake-videos-spread-facebook-tiktok-youtube-rcna101415 >accessed 6 June 2026

[12] Cosmina- Mihaela, Rosca, Adrian Stancu, and Emilian Marian Lovanovici,'The New Paradigm of Deepfake Detection at text level.' (2025), 15(5), Applied Sciences 2560 https://www.mdpi.com/2076-3417/15/5/2560 >accessed 7 June 2026

[13]The Indian Express, Taylor Swift AI 'deepfakes': What happened and where did the images come from?> accessed 7 June 2026

[14]BBC News, Deepfake of Zelensky circulating online (17 March 2022)> accessed 7 June 2026

[15] PaymentsJournal, It Happened! AI Deep Fake Mimicked a CEO's Voice and Stole €220,000 (4 October 2019)>accessed 8 June 2026.

[16] Ministry of Electronics and Information Technology, Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021> accessed 8 June 2026

[17] Ministry of Electronics and Information Technology, 'Inviting feedback/comments of stakeholders on the Draft amendments to Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules,2021- in relation to synthetically generated information' (22 October 2025)

1. Non-Consensual Intimate Imagery (NCII)

Deepfakes are frequently used to make fake, explicit videos or photos of people without their permission. Because these fakes look so real, victims often suffer from emotional distress, damaged reputations, and a massive invasion of their privacy.[12]

2. Political Misuse

Deepfakes can be used to spread lies, sway how the public thinks, and damage trust in democracy. When fake videos, speeches, or statements are wrongly blamed on political leaders, it confuses people and manipulates voters.[13]

3. Financial Fraud

Deepfakes can also facilitate financial crimes through identity impersonation and voice cloning. Criminals may imitate trusted individuals to obtain money, confidential information, or access to financial systems.[14]

5.6 INDIA'S CURRENT REGULATORY POSITION

India does not have a separate law specifically dealing with deepfakes. Instead, it regulates deepfake related issues through the Information Technology Act, 2000 and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules,2021.[15] Under Rule 3(1)(b), online platforms are required to prevent the spread of false, misleading, and impersonated content.In 2023 and 2024, the Ministry of Electronics and Information Technology (MeitY) issued advisories directing intermediaries to remove deepfake content, inform users about prohibited content,[16] and label AI-generated or synthetic content. The government has also proposed amendments to strengthen transparency, traceability, and accountability for AI-generated content.[17]

VI. CAN A PHOTO BE PROPERTY

DIGITAL IMAGES AS PROPERTY UNDER INDIAN LAW

6.1 CONCEPT OF PROPERTY

Property is not just about the physical object itself. Instead, it is about the legal rights to use it,

enjoy it, pass it on to others, and stop others from interfering with it.[18] Today, property law goes beyond physical things like land or goods. It also includes invisible things (intangible assets) like intellectual property, copyrights, patents, trademarks, and digital items.[19] Because of this, property law controls how these legal rights are created, used, transferred, and protected by the law.[21]

Historically, property was seen as anything a person could physically own, control, and hold. This early view was mostly limited to physical objects rather than a collection of legal rights. However, as society, business, and technology grew, the definition expanded to include non-physical items. Today, legal thinking has shifted from just looking at physical possession to focusing on ownership rights.[18,19]

According to legal expert Salmond, property is not the physical object itself. He explains that property is actually a legally protected interest. This interest gives the owner the right to possess, use, enjoy, transfer, and stop others from messing with it. This definition emphasizes that property is, at its core, a legal concept.[20,21]

6.2 HISTORY OF PROPERTY RIGHTS IN INDIA

The way people own property in India has changed completely over time. Originally, it shifted from local, community run traditions to a formal legal system shaped by British rule and later by India's own Constitution. Before the British arrived, property was managed through traditional social rules. Ownership wasn't usually tied to just one person; it was connected to community habits and social status.[22]A discussion on the evolution of property from tangible assets to informational assets. The Conceptual shift to intangible Property. Historically, property law protected physical possession. However, in the digital paradigm, a photograph shared online is an informational asset. Legal philosophers like John Locke argued that

[17]Ministry of Electronics and Information Technology, 'MeitY issues advisory to all intermediaries to comply with existing IT rules' (Press Information Bureau, 26 December 2023)
[18] Legal Services India, 'Definition & Concept of property'https://www.legalservicesindia.com/article/502/Definition-&-concept-of-property.html>accessed 8 June 2026
[19] University of Pittsburgh Law Blog, 'Introduction to Property Law: Understanding the Basics'https://online.law.pitt.edu/blog/introduction-to-property-law-understanding-the-basics>accessed 8 June 2026
[20]iPleaders Blog, 'Concept of Property' https://blog.ipleaders.in/concept-of-property/ >accessed 8 June 2026
[21] G. KANNIGA SHREE & DR. P.BRINDA, LAND PROVISION FOR THE LANDLESS, ILE PROPERTY AND LAND LAW REVIEW (ILE PLLR), 2 (1) of 2024, Pg. 07-15, APIS – 3920 – 0048 | ISSN - 2584-1998
[22] International Journal for Multidisciplinary Research (IJFMR), 'The Evolution of Right to Property: Exploring Pre and Post Constitutional https://www.ijfmr.com/papers/2024/4/25821.pdf >accessed 8 June 2026.

property rights are created when an individual mixes their labor with a resource. When a person captures an original photograph, they invest creative labor, establishing an intangible property interest in that digital asset.[6]

After winning independence, India created a constitution that first protected the right to property as a fundamental right under Articles 19(1)(f) and 31. However, this right quickly sparked fierce debates when the government started major land reforms to fight inequality and share land more fairly. Because of these battles, the 44th Constitutional Amendment of 1978 changed everything, it stripped property ownership of its fundamental right status and moved it to Article 300A as a standard constitutional or legal right. This was a massive shift that showed India was prioritizing social justice and fair resource sharing over absolute individual ownership.[23]

6.3 CONSTITUTIONAL POSITION

The Constitutional status of the Right to Property in India has changed significantly over time. Initially, it was recognised as a Fundamental Right under Articles 19(1)(f) and 31 of the Constitution. However, conflicts between individual property rights and government land reform policies led to the 44th Constitutional Amendment Act, 1978, which removed it from the list of Fundamental Rights.[24]

The amendment introduced Article 300A, which states that "no person shall be deprived of his property save by authority of law."[25] As a result, the Right to Property is now a constitutional and legal right rather than a Fundamental Right. This change was made to find a fair balance between protecting private ownership and supporting social justice and the general public's well-being.[26]

[23]Kumar Bal Govind Singh, 'The Right to Property in the Indian Constitution:Evolution and Impact' (SSRN,2023) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=447961>accessed 8 June 2026
[24]Ravindran, Rajesh Babu, Constitutional Right to property in Changing Times: The Indian Experience (September 13, 2012). Vienna Journal on International Constitutional Law, Vol.6, No. 2, 2012, Available at SSRN: https://ssrn.com/=2145845>accessed 8 June 2026
[25] International Journal for Multidisciplinary Research (IMMR), 'The Evolution of Right to Property: Exploring Pre and Post Constitutional Status'https://www.ijfmr.com/papers/2024/4/25821.pdf > accessed 9 June 2026
[26] Evolution History of Property Rights Through the Lens of Constitution Since Independence'(Legal Assist)https://legalassist.co.in/a-evolution-history-of-property-rights-through-the-lens-of-constitution-since-independence/ >accessed 9 June 2026
[27] Alliance School of Law, 'Decoding and Demystifying Deepfake Technology under Copyright Law' (Alliance University, 1 November 2025)https://www.alliance.edu.in/committees/acipr/blog/2025-11-01-decoding-and-demystifying-deepfake-technology-under-copyright-law.php >accessed 9 June 2026

6.4 WHY DOES TRANSFER OF PROPERTY ACT DOES NOT APPLY

In the digital age, the legal status of photos matters more than ever, especially with the rise of deepfakes. Even though photos can have huge personal and financial value, they are not considered "property" under The Transfer of Property Act, 1882. This specific law is meant to manage the transfer of physical and immovable property (like land or buildings); it was never designed to handle digital images or online content.[27]

Digital photographs are better understood as intangible assets that fall within the scope of intellectual property law, especially copyright law. Therefore, issues relating to the unauthorised use, manipulation, or reproduction of photographs are generally addressed through copyright, privacy, and personality rights rather than through traditional property law.[28] The emergence of deepfakes has further highlighted the limitations of conventional property laws, as they were not designed to deal with technologically generated misuse of digital identities and images.[27,28]

6.5 PROTECTION UNDER COPYRIGHT ACT,1957

The Copyright Act, 1957 offers indirect protection against the unauthorised use of photographs in deepfakes. Section 2(c) classifies photographs as artistic works, making them eligible for copyright protection. Section 13(1)(a) grants copyright protection to original artistic works, including photographs. Further, Section 14(c) provides the copyright owner with exclusive rights to reproduce, communicate, adapt, and distribute the work.[29] Section 51 states that copyright is infringed when a person, without the permission of the copyright owner, performs an act that is exclusively reserved for the owner under the Act. This provision may apply where

[28] International Journal of Law Reforms and Legal Studies, 'Deepfake Technology and it's Legal Implications' (2025) 5(4) https://ijlr.iledu.in/wp-content/uploads/2025/04/V5I453.pdf >accessed 9 June 2026
[29] Copyright Act, 1957 Explained' (LawSikho) https://lawsikho.com/blog/copyright-act-1957-explained> accessed 9 June 2026
[30] Are Indian Laws Equipped to Deal with Deepfakes?' (JILS Blog, National University of Juridical Sciences, 19 July 2020) https://jilsblognujs.wordpress.com/2020/07/19/are-indian-laws-equipped-to-deal-with-deepfakes/> accessed 10 June 2026
[31] Deepfake Regulation and Rights' (SCC Online Blog, 8 November 2025) https://www.scconline.com/blog/post/2025/11/08/deepfake-regulation-rights/ >accessed 10 June 2026
[32] Indian Journal of Legal Studies, 'Deepfake Technology and Legal Challenges' https://ijls.co.in/vol-iii-issue-16 >accessed 10 June 2026
[33] Kumar, Pankaj, Moral Rights under Section57 of the Indian Copyright Act,1957: An Expanded Analysis with Recent Developments, Waives, and Limitations (February 09, 2026). Available at SSRN:http://dx.doi.org/10.2139/ssrn.6201678>accessed on 11 June 2026

photographs are copied, manipulated, or used to create deepfakes without authorisation.

Additionally, Section 57 protects the author's moral rights by allowing them to claim authorship and object to any distortion, mutilation, or modification of their work that may harm their work that may harm their honour or reputation.[30] Therefore , creating or circulating deepfakes using a copyrighted photograph without permission may amount to copyright infringement and violation of moral rights.[31] However, the Act does not specifically regulate AI-generated deepfakes , which creates challenges in addressing emerging forms of digital misuse.[32]

6.6 MORAL RIGHTS

Section 57 of the Copyright Act, 1957 protects an author's moral rights independently of copyright ownership. These rights continue to exist even after the work has been assigned, transferred, or shared online. The provisions grants authors the right to claim authorship of their work and to object to any distortion, mutilation, modification, or other acts that may harm their honour or reputation.[33]

In the context of social media and deepfakes, uploading or sharing a photograph online does not result in the loss of moral rights. Therefore, if a person's photograph is manipulated or used to create a deepfake that damages the creator's reputation, protection may be sought under Section 57. The Delhi High Court in Amar Nath Sehgal v Union of India also recognised that moral rights continue to survive independently of economic rights and emphasised the protection of the integrity of creative works.[34] [8]

6.7 WIPO COPYRIGHT TREATY

Digital works are protected at the international level through the WIPO Copyright Treaty (WCT), 1996, which was adopted to address copyright issues arising in the digital environment The treaty extends copyright protection to online and digital works. Article 6 grants authors the exclusive right to authorise the distribution of their works, and Article 8 grants authors the

[34] Amar Nath Sehgal v Union of India (2005) 30 PTC 253 (Del).
[35] WIPO Copyright Treaty (WCT) https://www.wipo.int/en/web/treaties/ip/wct/index > 11 June 2026
[36] Guide to the Berne Convention for the Protection of Literary and Artistic Works https://www.wipo.int/edocs/pubdocs/en/wipo_pub_226.pdf.> 11 June 2026
[37] ICC Development (International) Ltd v Arvee Enterprises 2003 (26) PTC 245 (Del).
[38] Titan Industries Ltd v Ramkumar Jewellers 2012 SCC Online Del 2382.

right to communicate their works to the public, including making them available through digital networks.[35]

In addition, the Berne Convention for the Protection of Literary and Artistic Works ensures that creators receive copyright protection in all member countries without requiring separate registration. Article 5(2) of the convention provides that the enjoyment and exercise of copyright shall not be subject to any formality, meaning that protection is automatic once the work is created.[36] Together, these interns instruments recognise that digital creations shared online deserve the same legal protection as traditional creative works and require safeguards against unauthorised use and technological misuse.

6.8 PERSONALITY RIGHTS AND RIGHT TO IMAGE

Personality rights protect an individual's identity, including their name, image, likeness, voice, and other identifiable characteristics from unauthorized use. These rights belong only to real people, giving them the power to control and make money from their own identity.[37]

Specifically, image rights allow a person to decide how their photos and visual identity are used. When it comes to social media and deepfakes, just because you upload a photo online does not mean you are giving everything else free permission to copy, change, or exploit it.[38]

The courts have backed this up in a couple of major cases. The Delhi High Court made it clear in the case of ICC Development v Arvee Enterprises that these "personality rights" belong strictly to living individuals, not to corporations or organized events. And in Titan Industries Ltd v. Ramkumar Jewellers case the court ruled that using someone's image without permission is a misuse of their personality rights because it falsely makes people think that person is endorsing a product.[9]

VII. IP, PRIVACY, AND PERSONALITY RIGHTS

VIOLATION OF INTELLECTUAL PROPERTY, PRIVACY AND PERSONALITY RIGHTS

[39] A Study on Deepfakes and Copyright Infringement, International Journal of Law Management & Humanities, https://ijlmh.com/paper/a-study-on-deepfakes-and-copyright-infringement/ >accessed 12 June 2026
[40] Griffith Barbee, 'The Impact of Deepfake Technology on Copyright Infringement Claims' (2023), https://griffithbarbee.com/the-impact-of-deepfake-technology-on-copyright-infringement-claims/ >accessed 12 June 2026

7.1 COPYRIGHT INFRINGEMENT THROUGH DEEPFAKES

The proliferation of synthetic media poses profound challenges to the copyright enforcement regime. Furthermore, the decentralized nature of deepfake creation obfuscates the determination of liability, as authorship is distributed across AI developers, end-users, and platform hosts.[39]

A problem is that deepfakes copy and change original works without permission. By digitally copying a person's look, voice, or creative work, deepfakes can create new versions (known as derivative works) that look and sound just like the original, all without the creator's consent. This violates the exclusive rights that copyright holders are supposed to have for their own creations.[40] In India, these actions can break Section 14 of the Copyright Act, 1957, which protects an owner's right to copy, adapt, or share their copyrighted work. On top of that, deepfakes make it very hard to blame any single person under the law, since making them usually involves many different groups, including AI developers, the people using the software, and the online platforms where they are shared.

Deepfakes also complicate the process of assigning legal responsibility because their creation often involves multiple actors, including AI developers, users, and online platforms. As a result, identifying the person accountable for copyright violations becomes increasingly difficult.[10] Furthermore, the widespread circulation of deepfakes may reduce the economic and reputational value of original works by blurring the distinction between authentic and manipulated content. The unauthorised use and dissemination of copyrighted material through deepfakes may therefore constitute infringement under Section 51 of the Copyright Act, 1957.

7.2 RIGHT TO PRIVACY UNDER ARTICLE 21

The Indian Constitution does not explicitly recognise the right to privacy as a fundamental right. However, through judicial interpretation, the Supreme Court gradually incorporated it within the scope of the right to like and personal liberty under Article 21. The right to privacy protects an individual's dignity,autonomy and freedom from unnecessary interference.[41]

[38] Titan Industries Ltd v Ramkumar Jewellers 2012 SCC Online Del 2382.
[39] A Study on Deepfakes and Copyright Infringement, International Journal of Law Management & Humanities, https://ijlmh.com/paper/a-study-on-deepfakes-and-copyright-infringement/ >accessed 12 June 2026
[40] Griffith Barbee, 'The Impact of Deepfake Technology on Copyright Infringement Claims' (2023), https://griffithbarbee.com/the-impact-of-deepfake-technology-on-copyright-infringement-claims/ >accessed 12 June 2026

Its development began in Kharak Singh v. State of Uttar Pradesh (1962), where the Court recognised privacy as an important aspect of personal liberty. This principle was further expanded in Gobind v. State of Madhya Pradesh (1975) and R. Rajagopal v. State of Tamil Nadu (1994), which described privacy as the "right to be let alone" and extended protection to personal matters such as family life, marriage and procreation.[42]

The position was conclusively settled in Justice K.S. Puttaswamy v. Union of India (2017), where the Supreme Court declared that the right to privacy is an intrinsic part of Article 21 and other fundamental rights under Part III of the Constitution, while also clarifying that it is subject to reasonable restrictions.

7.3 INFORMATIONAL PRIVACY

In Justice K.S. Puttaswamy (Retd.) v. Union of India (2017), the Supreme Court of India unanimously recognised the right to privacy as a fundamental right under Article 14, 19 and 21 of the Constitution. The Court held that privacy includes informational privacy, which gives individuals control over their personal data and how it is collected, used and shared.[43]

The Judgement also emphasised an individual's right to control their own identity and image. This means that a person's photograph, facial features, biometric information and other personal attributes cannot be collected, reproduced or used without their informed consent, except in accordance with a valid law. The Court acknowledged that in the digital age, misuse of a person's image can threaten individual autonomy, dignity and personal liberty. Therefore, adequate safeguards and data protection measures are essential to prevent unauthorised exploitation of personal information.

7.4 UNIVERSAL DECLARATION OF HUMAN RIGHTS (UDHR) & INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS

Article 12 of the UDHR protects individuals from arbitrary interference with their privacy, family, home, correspondence, honour and reputation. It states that every person has the right to legal protection against such interference or attacks. This provision establishes privacy as a

[41]Kharak Singh v State of Uttar Pradesh AIR 1963 SC 1295, available at:https://indiankanoon.org/doc/1199182/.
[42] Kush Kalra, 'Right to Privacy under Indian Constitution' (2020) GIBS Law Journal, Vol 2 No, available at:https://gitarattan.edu.in/wp-content/uploads/2020/11/giBS-Law-Journal-2020-Research-Paper-5.pdf
[43] Justice *K.S.* Puttaswamy (Retd.) and Anr. V Union of India and Ors., (2017) 10 SCC 1 (Supreme Court of India).

fundamental human right and safeguards an individual's personal identity and dignity from unlawful intrusion.[44]

Article 17 of the ICCPR prohibits arbitrary or unlawful interference with a person's privacy, family, home or correspondence, and protects individuals against unlawful attacks on their honour and reputation. It also obligates States to provide legal protection against such violations. This article strengthens international recognition of privacy rights and places a duty on governments to protect personal information and individual autonomy.[45]

7.5 INFORMATIONAL TECHNOLOGY ACT, 2000

Section 66E of the Information Technology Act, 2000 criminalises the intentional capture, publication or electronic transmission of images of a person's private areas without their consent in circumstances that violate their privacy. The provision recognises an individual's reasonable expectation of privacy and prescribes punishment of imprisonment up to three years, a fine up to ₹2 lakh, or both.[46]

The increasing use of digital platforms has led to a rise in cases involving the non-consensual sharing of intimate images. Karnataka Police have clarified that consent to record an image does not amount to consent to publish or distribute it. Any unauthorised sharing of obscene or private images should be treated as a cognisance offence, and police are required to register an FIR and take appropriate legal action.[47]

7.6 BHARATIYA NYAYA SANHITA, 2023

Deepfake technology can facilitate offences such as voyeurism and cyberstalking by enabling the creation and circulation of manipulated images and videos without a person's consent. Under Section 77 of the Bharatiya Nyaya Sanhita (BNS), voyeurism includes capturing, watching or disseminating images of a woman engaged in a private act where she has a reasonable expectation of privacy. Even if a woman consents to the recording of an image, sharing or distributing it without her consent constitutes an offence.[48] In the context of

[44] Universal Declaration of Human Rights, adopted 10 December 1948, UNGA Res 217 A (III), art. 12.
[45] International Covenant on Civil and Political Rights, adopted 16 December 1966, 999 UNITS 171, art. 17.
[46] Information Technology Act, 2000, s. 66E
[47] Consent to record no licence to share; FIRs a must in obscene image leak cases: Karnataka Police, The Times of India, 12 June 2025, https://timesofindia.indiatimes.com/city/bengaluru/consent-to-record-no-licence-to-share-firs-a-must-in-obscene-image-leak-cases-karnataka-police/articleshow/131805260.cms.> accessed 13 June 2026

deepfakes, digitally altered intimate images or videos can amount to voyeuristic abuse when they are created or circulated to violate an individual's privacy.[49]

Section 78 of the BNS criminalises stalking, including monitoring a woman's activities through the Internet, email or other forms of electronic communication.[48] Synthetic media exacerbates the gravity of cyberstalking, providing perpetrators with the utility to orchestrate targeted harassment, identity impersonation, and sustained psychological distress. This causes deep emotional distress, ruins, reputations, and creates constant fear. Because of this, it is crucial to quickly gather digital evidence and step in legally to stop these crimes.[50]

7.7 PERSONALITY RIGHTS AS EVOLVING TORTS

Deepfakes have made worries about personality rights much worse. They allow people to use someone else's photos, voice, face, and identity without permission to make money,pretend to be them, or damage their reputation. Even though India does not have a specific law just for personality rights, courts have ruled that these protections naturally grow out of the rights to privacy and publicity.

In the 2003 case ICC Development (International) Ltd. v. Arvee Enterprises, the Delhi High Court noted that the right to publicity comes from the right to privacy and belongs mostly to the individual. The court ruled that no one can use a person's name, image, signature, voice, or other unique traits to make money without their permission. In ICC Development (International) Ltd. v. Arvee Enterprises (2003), the Delhi High Court observed that the right of publicity originates from the right to privacy and primarily belongs to an individual. It held that a person's name, image, signature voice and other identifiable attributes cannot be commercially exploited without authorisation.[51] This principle has become increasingly relevant in the context of deepfakes, where artificial intelligence can replicate an individual's identity without consent.

Because of this, deepfakes can be treated as a new kind of civil wrong (or tort) for violating personality rights. They allow people's digital identities to be misused, which causes damaged reputations, emotional suffering, and a loss of personal control. Since India lacks a specific law for this, there is a clear need to build stronger legal protections against unauthorised, AI-

generated impersonation.[13]

7.8 Free Speech v Privacy

Deepfakes create a conflict between the right to freedom of speech and expression under Article 19(1)(a) and the right to privacy under Article 21 of the Indian Constitution. While AI-generated content can be used for legitimate purposes such as creativity, satire and education, it can also be misused to spread misinformation, impersonate individuals and violate privacy.

Regulating deepfakes therefore requires a balanced approach. Over-regulation may restrict innovation and free expression, whereas inadequate regulation may expose individuals to reputational harm, identity theft and privacy violations. Any new laws should focus on stopping harmful deepfakes made without permission, while still protecting free speech and creative expression.[52]

7.9 GAPS IN LAWS

No laws in India specifically mention deepfakes. Instead, the country uses older, existing rules under the Information Technology Act, standard criminal laws, and social media platform guidelines to deal with the harms caused by AI.[53] In contrast, the European Union (EU) AI Act has a dedicated law that categorises and regulates artificial intelligence based on how risky it is.

India also does not require companies to label deepfakes responsible, and has no overall system to monitor AI. While the EU AI Act forces companies to be transparent, check for risks, and follow strict rules, India's approach is mostly reactive- meaning it only deals with the damage after it has already happened.

[48]Bharatiya Nyaya Sanhita, 2023, ss. 77–78.
[49]Law Journals, "Deepfakes and Emerging Challenges to Privacy and Criminal Law", Vol. 12, Issue 1(2026), https://www.lawjournals.org/assets/archives/2026/vol12issue1/12074.pdf.
[50]Indian Journal of Law and Legal Research, "Section 78 BNS: Cyberstalking, Gender and Digital Evidence in Contemporary India",https://www.ijllr.com/post/section-78-bns-cyberstalking-gender-and-digital-evidence-in-contemporary-india.
[51] ICC Development (International) Ltd. v, Arvee Enterprises and Anr., 2003(26) PTC 245 (Del).
[52] Deepfake Regulation vs Free Speech: Should India Criminalise AI-Generated Deepfakes Under Fundamental Rights Concerns? LawVS, https://lawvs.com/articles/deepfake-regulation-vs-free-speech-should-india-criminalize-ai-generated-deepfakes-under-fundamental-rights-concerns>accessed 13 June 2026
[53] The Face of Fraud: A Comparative Analysis of Deepfake Regulations in the EU AI Act v India's IT Rules, IJIRT(2026), https://ijirt.org/publishedpaper/IJIRT191410_PAPER.pdf.> 13 June 2026

VIII. WHO IS LIABLE

DETERMINATION OF LIABILITY

8.1 FRAMING THE LIABILITY QUESTION

Making and sharing deepfakes is rarely done by just one person. Usually, one person creates the fake media using free software, and then a social media platform acts as the tool to spread it to a massive audience. This involvement of two different parties raises a tough legal question: should the platform that hosted and shared it also be held responsible for the damage? The next section will look at creator liability and platform liability separately under Indian law, and then explain when both parties might share the blame.

8.2 CREATOR LIABILITY

STATUTORY PROVISIONS	**OFFENCE**	**PUNISHMENT**
Section 66C, IT Act,2000	Identity theft using electronic means	Up to 3 years imprisonment + Fine Up to ₹1 Lakh
Section 66E, IT Act,2000	Capturing/Publishing Private images without consent	Up to 3 years imprisonment + Fine Up to ₹2 Lakhs
Section 67, IT Act,2000	Publishing Obscene Material Electronically	Up to 3 years imprisonment (first conviction)+ Fine
Section 67A, IT Act,2000	Publishing Sexually explicit material	Up to 5 years imprisonment + Fine Up to ₹10 Lakhs
Section 77, BNS,2023	Voyeurism	Up to 3 years imprisonment + Fine
Section 316, BNS,2023	Cheating by impersonation	Up to 5 years imprisonment + Fine
Section 51, Copyright Act,1957	Infringement of Copyright	Civil remedies+ Criminal Liability under Section 63

8.3 PLATFORM LIABILITY

Section 79 of the Information Technology Act, 2000 provides social media platforms with conditional immunity from liability for content posted by third-party users. Under Section 79(1), an intermediary is not liable for any information made available by it, provided its role is limited to that of a facilitator rather than a publisher. However, this protection is not absolute. Section 79(2) requires the intermediary to observe due diligence and to refrain from initiating, selecting, or modifying the transmitted content. Section 79(3) further provides that safe harbour is withdrawn where the intermediary has actual knowledge of unlawful content, including deepfake material violating an individual's rights, and fails to expeditiously remove or disable access to it upon receiving such knowledge or a notification from the appropriate government authority. [15]

8.4 THE ACTUAL KNOWLEDGE STANDARD

In the case Shreya Singhal v. Union of India, the Supreme Court set up the rule of "actual knowledge" when deciding when online platforms (intermediaries) are responsible for user content under the Information Technology Act, 2000. The Court ruled that websites and apps do not have to constantly watch everything users post. Instead, they can only be forced to take down illegal content after they receive an official court order or a notice from an authorised government agency.[57]

When it comes to deepfakes, this rule causes big real-world problems. Harmful AI-generated content can spread incredibly fast before a platform ever receives official notice about it. This delay in finding and deleting the fakes can lead to broken privacy, ruined reputations, and the massive spread of lies.

8.5 IT RULES 2021 AND MeitY ADVISORY

Rules 3 and 4 of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 impose due diligence obligations on intermediaries and significant social media intermediaries. Platforms are required to establish grievance redressal mechanisms, remove content involving impersonation, sexually explicit material and

[54] Information Technology Act, 2000, S 67A, 79, 79(1),79(2),79(3)
[55] Bharatiya Nyaya Sanhita, 2023, S 77,316
[56] Copyright Act, 1957, S 51

artificially morphed images, and appoint compliance officers and publish transparency reports.[58]

In its 26 December 2023 advisory, the Ministry of Electronics and Information Technology (MeitY) directed intermediaries to take proactive measures against deepfakes by informing users about prohibited content and ensuring compliance with existing laws. The advisory reinforced platform accountability by requiring timely action against AI- generated misinformation, impersonation and privacy violations.[59]

8.6 ESTABLISHING LIABILITY

Deepfake related harm on social media may attract liability for both creators and platforms. The creator bears primary liability because the author 's use of a person's image, voice or identity can violate privacy, personality rights and copyright rights.

Social media platforms may incur secondary liability if they fail to comply with their due diligence obligations. Under Section 79 of the Information Technology Act,2000, intermediaries lose safe harbour protection when they have actual knowledge of unlawful deepfake content and fail to remove it. Therefore, legal responsibility may be imposed on both creators and in certain circumstances, on platforms that facilitate the dissemination of harmful deepfake content.

IX. REMEDIES AVAILABLE

LEGAL REMEDIES AND THEIR ADEQUACY

9.1 CIVIL AND CRIMINAL REMEDIES

Victims of deepfakes may seek civil remedies such as injunctions to restrain the creation publication or circulation of harmful content and claim damages for copyright infringement and tortious harm, including reputational injury and misuse of identity.[60, 61]

They may also pursue criminal remedies by filing an FIR under the Information Technology

[57] Shreya Singhal v Union of India, (2015) 5 SCC 1
[58] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules,2021, r.3., r.4
[59] Ministry of Electronics and Information Technology (MeitY),Advisory to Intermediaries on Deepfakes and AI-generated Content, 26 December 2023,https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=1990542&reg=48&lang=2.

Act, 2000 and the Bharatiya Nyaya Sanhita, 2023 for offences such as identity theft, voyeurism, obscenity, impersonation and privacy violations.[62]

However, enforcing these remedies remains challenging. Victims often face delays in registering FIRs, difficulties in identifying anonymous creators, jurisdictional issues and problems in collecting digital evidence. The rapid spread of deepfakes across multiple platforms also makes proving authorship and preventing further dissemination difficult.[63,64]

9.2 Platform Greiveance Mechanism

Rule 3(2) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 requires intermediaries to establish a grievance redressal mechanism and appoint a grievance Officer whose contact details must be published on the platform. The Grievance Officer is responsible for acknowledging complaints within 24 hours and resolving them within a prescribed time frame.

Rule 4(4) places additional obligations on significant social media intermediaries by requiring them to remove or disable access, within 24 hours of receiving a complaint, to content exposing an individual's private areas, depicting nudity, sexual acts, impersonation or non-consensual intimate imagery (NCII). These provisions are particularly relevant to deepfakes, as AI-generated intimate images and videos can cause severe privacy, reputational and psychological harm. They provide victims with a faster complaint and takedown mechanism and strengthen platform accountability in addressing the spread of harmful deepfake content.

9.3 ASSESSMENT OF ADEQUACY

Despite multiple legal provisions, India still lacks a comprehensive framework to address deepfakes effectively. The statutory landscape reveals three systematic lacunae. First, India

[60] Deepfake Injunctions India, Global Law Experts, https://globallawexperts.com/deepfake-injunctions-india/ >accessed 14 June 2025
[61] Is the Indian Law Equipped Enough to Deal with Deepfakes?, iPleaders https://blog.ipleaders.in/is-the-indian-law-equipped-enough-to-deal-with-deepfakes/ >accessed 14 June 2026
[62]Information Technology Act, 2000; Bharatiya Nyaya Sanhita, 2023.
[63]Regulating Deepfake Technology: Ethical and Legal Challenges under Indian Law, Parujanwala Law Academy, available at:https://www.pahujalawacademy.com/regulating-deepfake-technology-ethical-and-legal-challenges-under-indian-law >accessed 15 June 2025
[64]IT Rules 2026: Deepfake Takedown, 3 Hour Rate and AI Labelling Explained, LawSikho, available at: https://lawsikho.com/blog/it-rules-2026-deepfake-takedown-3-hour-rule-and-ai-labelling-explained/ >accessed 15 June 2026

lacks dedicated legislative frameworks regulating synthetic media; instead, it relies on a fragmented patchwork of provisions under the IT Act and the BNS that merely address consequential injuries rather than regulating the generative technology architecture itself.[65]

Second, the criminal justice process is often too slow and hard to enforce. Victims frequently face delays when trying to file a First Information Report (FIR), Tracy down anonymous creators, gather digital evidence, and prove who actually made the video. This lag allows harmful content to spread incredibly fast before any real legal action can stop it.[66]

Third, online platforms handle the problem inconsistently. Social media companies generally only take action after someone complains or after they receive official notice of illegal content. This results in major delays in deleting harmful deepfakes and leaves victims unprotected.

In contrast, the Online Safety Act, 2023 takes a much more aggressive approach by forcing online platforms to actively find, reduce, and remove harmful content. This provides a great model for how India could regulate deepfakes in the future. [67]

9.4 IMPACT ON VICTIMS

Deepfakes have significant ethical implications as they can damage an individual's reputation, mental health and livelihood. The unauthorised use of a person's image, voice or identity may lead to humiliation, emotional distress, anxiety and loss of public trust. In some cases, victims may also suffer professional and economic consequences due to the rapid circulation of false or misleading content.[68]

The risks associated with deepfakes extend beyond private individuals and can affect public figures, institutions and democratic processes.

X. REFORM SUGGESTIONS

[65] Information Technology Act, 2000; Bharatiya Nyaya Sanhita, 2023; Copyright Act,1957; Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
[66] The Indian Law Equipped Enough to Deal with Deepfakes ?, iPleaders, https://blog.ipleaders.in/is-the-indian-law-equipped-enough-to-deal-with-deepfakes/.>accessed 15 June 2026
[67] Online Safety Act, 2023.
[68] Regulating Deepfake Technology: Ethical and Legal Challenges under Indian Law, Parujanwala Law Academy.https://www.pahujalawacademy.com/regulating-deepfake-technology-ethical-and-legal-challenges-under-indian-law.>accessed 15 June 2026

10.1 NEED FOR REFORM

India's current laws only deal with deepfake problems indirectly and after the damage is already done. Older laws like the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, and the Copyright Act, 1957 were never meant to regulate AI-generated fake media. As pointed out in Chapters IV and VI, the biggest gaps are the lack of a specific law, no rules requiring deepfakes to be labelled, slow legal enforcement, and inconsistent actions by social media platforms. These weaknesses show that India urgently needs focused changes to its laws and legal procedures.

10.2 DEDICATED DEEPFAKE LEGISLATION

India needs to either create a new law just for deepfakes or update the Information Technology Act, 2000. This change should clearly define what a "deepfake" or "synthetically generated content" actually is. Instead of using unrelated laws to punish these actions, the government should set up a tiered system where punishments match the seriousness of the crime. For example, specific penalties should be tailored for different categories like making fake adult content without permission, spreading fake political news, and using fake identities to steal money online.

10.3 INSTITUTIONALIZING CRYPTOGRAPHIC WATERMARKING PROTOCOLS

Rather than replying on non-binding executive advisories such as the MeitY advisory of March 2024 India must establish a statutory mandate for synthetic media provenance this can be achieved by amending Rule 3(1)(b) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules,2021. The amendment should impose an affirmative duty on AI developers and generative platforms to embed immutable, cryptographic metadata (such as C2PA standards) at the architectural layer. Failure to do so should strip developers of any potential liability exemptions and categorise non-complaint software as inherently hazardous digital infrastructure.

10.4 TRANSITIONING FROM REACTIVE TO PROACTIVE DUTY OF CARE

India's current safe-harbour architecture under Section 79 of the IT Act remains strictly reactive, contingent upon the "actual knowledge" standard crystallised in Shreya Singhal v. Union of India. To mitigate the viral velocity of deepfakes, this paradigm must shift toward a

proactive "duty of care," mirroring Section 19 of the UK Online Safety Act, 2023. Significant Social Media Intermediaries (SSMIs) must be legally required to deploy automated, algorithmic scanning tools trained to flag known non-consensual intimate imagery (NCII) signatures at the point of ingest, moving away from a post reporting takedown mechanism.

10.5 SPECIAL ADJUDICATORY FRAMEWORKS UNDER THE E-COURTS MISSION MODE PROJECT

The demand for expedited remedies cannot be met by simply calling for "fast-track courts". Instead, the Phase III of the E-courts Mission Mode Project must be leveraged to create dedicated, digitally native tribunals specialising in synthetic media litigation. Under Section 46 of the IT Act, 2000, the Central Government appoints Adjudicating Officers. These offices must be scaled up into fully integrated cyber-tribunals. These tribunals should be explicitly empowered to issue ex-parts ad-interim take down injunctions within a statutory window of 24 hours upon a prima facts pie demonstration of non-consensual deepfake deployment.

10.6 AWARENESS AND IMPLEMENTATIONS

Changing the laws isn't enough. We also have to make sure they actually work in real life. We need to teach the public, especially women and young people, how to report deepfakes and where to get help. To make this happen, we need dedicated helplines, free legal aid, well-trained cybercrime police, and regular checks to ensure social media platforms are following the rules. In the end, new laws will only succeed if we have strong enforcement and an informed public.

XI. CONCLUSION

The Study shows that the person actually making the deepfake is the one most to blame under the law. Because they made and shared the AI content without permission, they can be held responsible for stealing copyright, invading privacy and violating personality rights. Their actions can break several Indian laws, including the Information Technology Act (2000), the Bharatiya Nyaya Sanhita (2023), and the Copyright Act (1957). Social media platforms can also get into legal trouble, but usually only if they fail to follow basic safety rules, or if they are told about a harmful deepfake and refuse to take it down, which causes them to lose their legal immunity (known as "safe harbour" protection) under Section 79 of the Information

Technology Act. Even though victims can try to use civil lawsuits, police complaints, or platform reporting tools to get help, they still face massive hurdles because legal action is incredibly slow, platforms handle complaints inconsistently, and India lacks a specific law built for this problem.

Ultimately, the study proves that using someone's image for a deepfake without their consent actively violates their privacy, copyright, and identity rights. The blame falls first on the creator, and second on the social media platform if it helps spread the content without stepping in. Right now, India's legal system only reacts after the damage is already done instead of preventing it from happening. Because deepfake technology is evolving so fast, India urgently needs specific laws, rules that force creators to label AI content, stricter rules for platforms, faster ways for victims to get help, and better public education. If these changes aren't made soon, the law will fall further and further behind technology, leaving ordinary people unprotected against digital harms the legal system was never built to handle.

REFERENCES

A. STATUTES AND RULES

1. Constitution of India,1950, art 14, 19,21 and 300A
2. Transfer of property Act, 1882
3. Copyright Act, 1957, ss 2(c), 13(1)(a), 14(c), 51, 57
4. Information Technology Act, 2000, ss 66C, 66E, 67, 67A,79
5. Bharatiya Nyaya Sanhita, 2023, ss 77, 78, 316
6. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, rr 3(1)(b), 3(2), 4(4).
7. WIPO Copyright Treaty, 1996,arts 6,8
8. Berne Convention for the protection of Literary and Artistic works, 1886(as revised), art 5(2).
9. Universal Declaration of Human Rights, 1948, art 12
10. International Covenent on Civil and Political Rights 1966, art 17
11. Regulation (EU) 2024/1689 Artificial Intelligence Act[2024], art 50
12. Online Safety Act,2023 (UK)

B. CASES

1. Justice K.S. Puttaswamy (Retd.) v Union of India (2017) 10 SCC 1
2. Shreya Singhal v Union of India (2015) 5 SCC 1
3. Kharak Singh v State of Uttar Pradesh AIR 1963 SC 1295
4. Gobind v State of Madhya Pradesh (1975) 2 SCC 148
5. R Rajagopal v State of Tamil Nadu (1994) 6 SCC 632
6. Amar Nath Sehgal v Union of India 2005 (30) PTC 253 (Del)
7. Titan Industries Ltd v Ramkumar Jewellers 2012 (50) PTC 486 (Del)

C. GOVERNMENT ADVISORIES

1. Ministry of Electronics and Information Technology, Advisory to All Intermediaries to Comply with Existing IT Rules (26 December 2023)

2. Ministry of Electronics and Information Technology, Advisory on Misinformation and Deepfake Mandating Unique Metadata (1 March 2024)

D. ARTICLES AND REPORTS

1. Bhale, Swanand, Deepfake Laws in India: The Need for Legal Regulation in the AI Era(February01,2025).Available at SSRN:http://dx.doi.org/10.2139/ssrn.5153296 > accessed 3 June 2026

2. R, Sarferaaz Khaan, Countering Deepfakes: A Strategic Blueprint for Modernizing Indian Criminal Law (November 27,2025). International Journal for Legal Research and Analysis, Volume 2, Pp. 6-7, Available at SSRN:http://dx.doi.org/10.2139/ssrn.591854> accessed 3 June 2026

3. ADABALA, DIMPLE SAHITHI, When Technology Lies: Deepfake and Criminal Law in India (April 28, 2026). Available at SSRN:http://dx.doi.org/10.2139/ssrn.6665081 > accessed 3 June 2026

4. Thakur, Dushyant Singh, Deepfakes as Human Rights Violations: Rethinking Dignity and Privacy in India (September 10, 2025). Available at SSRN:http://dx.doi.org/10.2139/ssrn.5532383 > accessed 3 June 2026

5. Farish, Kelsey, Do Deepfakes Pose a Golden Opportunity Considering Whether English Law Should Adopt California's Publicity Right in the Age of the Deepfake (September 1, 2019). Available at SSRN:http://dx.doi.org/10.2139/ssrn.3648960 >accessed 3 June 2026

6. Priyanshu Yadav, Stolen Faces, Borrowed Voices: The Legal Imperative for Regulating Deepfake in India,DOI: https://doij.org/10.10000/IJLMH.1111413> accessed 3 June 2026

7. Daniel Miller, Klaire Somoray and Hallev Stevens, A Shallow History of Deepfakes, Pp.2-16. Available at SSRN:https://dx.doi.org/10.2139/ssrn.5130379>accessed 4 June 2026

8. BBC News, 'Deepfake of Zelensky circulating online'(BBC News, 17 March 2022)https://www.bbc.com/news/technology-60780142 >accessed 6 June 2026.

9. SentinelOne, 'Deepfakes: Definition, Types, and Key Examples (16 July2025) https://www.sentinelone.com/cybersecurity-101/cybersecurity/deepfakes/ >accessed 6

June 2025

10. CyberPeace Foundation, 'The Efforts of Social Media Platforms to Counter Deepfake(CyberPeace, n.d.)https://www.cyberpeace.org/resources/blogs/the-efforts-of-social-media-platforms-to-counter-deepfake >accessed 6 June 2026

11. NBC News, 'Deepfake scams have arrived on Facebook, TikTok and YouTube' (NBC News,n.d.)https://www.nbcnews.com/tech/tech-news/deepfake-scams-arrived-fake-videos-spread-facebook-tiktok-youtube-rcna101415 >accessed 6 June 2026

12. Cosmina- Mihaela, Rosca, Adrian Stancu, and Emilian Marian Lovanovici,'The New Paradigm of Deepfake Detection at text level.' (2025), 15(5), Applied Sciences 2560 https://www.mdpi.com/2076-3417/15/5/2560 >accessed 7 June 2026

13. The Indian Express, Taylor Swift AI 'deepfakes': What happened and where did the images come from?> accessed 7 June 2026

14. BBC News, Deepfake of Zelensky circulating online (17 March 2022)> accessed 7 June 2026

15. PaymentsJournal It Happened! AI Deep Fake Mimicked a CEO's Voice and Stole €220,000 (4 October 2019)>accessed 8 June 2026.

16. Legal Services India, 'Definition & Concept of property'https://www.legalservicesindia.com/article/502/Definition-&-concept-of-property.html >accessed 8 June 2026

17. University of Pittsburgh Law Blog, 'Introduction to Property Law: Understanding the Basics'https://online.law.pitt.edu/blog/introduction-to-property-law-understanding-the-basics>accessed 8 June 2026

18. iPleaders Blog, 'Concept of Property' https://blog.ipleaders.in/concept-of-property/ >accessed 8 June 2026

19. International Journal for Multidisciplinary Research (IJFMR), 'The Evolution of Right to Property: Exploring Pre and Post Constitutional https://www.ijfmr.com/papers/2024/4/25821.pdf >accessed 8 June 2026.

20. Kumar Bal Govind Singh, 'The Right to Property in the Indian Constitution:Evolution and Impact' (SSRN,2023) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=447961>accessed 8 June 2026

21. Ravindran, Rajesh Babu, Constitutional Right to property in Changing Times: The Indian Experience (September 13, 2012). Vienna Journal on International

Constitutional Law, Vol.6, No. 2, 2012, Available at SSRN: https://ssrn.com/=2145845>accessed 8 June 2026

22. International Journal for Multidisciplinary Research (IMMR), 'The Evolution of Right to Property: Exploring Pre and Post Constitutional Status'https://www.ijfmr.com/papers/2024/4/25821.pdf > accessed 9 June 2026

23. Evolution History of Property Rights Through the Lens of Constitution Since Independence'(Legal Assist)https://legalassist.co.in/a-evolution-history-of-property-rights-through-the-lens-of-constitution-since-independence/ >accessed 9 June 2026

24. Alliance School of Law, 'Decoding and Demystifying Deepfake Technology under Copyright Law' (Alliance University, 1 November 2025)https://www.alliance.edu.in/committees/acipr/blog/2025-11-01-decoding-and-demystifying-deepfake-technology-under-copyright-law.php >accessed 9 June 2026

25. International Journal of Law Reforms and Legal Studies, 'Deepfake Technology and it's Legal Implications' (2025) 5(4) https://ijlr.iledu.in/wp-content/uploads/2025/04/V5I453.pdf >accessed 9 June 2026

26. Copyright Act, 1957 Explained' (LawSikho) https://lawsikho.com/blog/copyright-act-1957-explained >accessed 9 June 2026

27. Are Indian Laws Equipped to Deal with Deepfakes?' (JILS Blog, National University of Juridical Sciences, 19 July 2020) https://jilsblognujs.wordpress.com/2020/07/19/are-indian-laws-equipped-to-deal-with-deepfakes/ >accessed 10 June 2026

28. Deepfake Regulation and Rights' (SCC Online Blog, 8 November 2025) https://www.scconline.com/blog/post/2025/11/08/deepfake-regulation-rights/ >accessed 10 June 2026

29. Indian Journal of Legal Studies, 'Deepfake Technology and Legal Challenges' https://ijls.co.in/vol-iii-issue-16 >accessed 10 June 2026

30. Kumar, Pankaj, Moral Rights under Section57 of the Indian Copyright Act,1957: An Expanded Analysis with Recent Developments, Waives, and Limitations (February 09, 2026). Available at SSRN:http://dx.doi.org/10.2139/ssrn.6201678>accessed on 11 June 2026

31. A Study on Deepfakes and Copyright Infringement, International Journal of Law Management & Humanities, https://ijlmh.com/paper/a-study-on-deepfakes-and-copyright-infringement/ >accessed 12 June 2026

32. Griffith Barbee, 'The Impact of Deepfake Technology on Copyright Infringement Claims' (2023), https://griffithbarbee.com/the-impact-of-deepfake-technology-on-

copyright-infringement-claims/ >accessed 12 June 2026

33. Kush Kalra, 'Right to Privacy under Indian Constitution' (2020) GIBS Law Journal, Vol 2 No, available at:https://gitarattan.edu.in/wp-content/uploads/2020/11/giBS-Law-Journal-2020-Research-Paper-5.pdf

34. Consent to record no licence to share; FIRs a must in obscene image leak cases: Karnataka Police, The Times of India, 12 June 2025, https://timesofindia.indiatimes.com/city/bengaluru/consent-to-record-no-licence-to-share-firs-a-must-in-obscene-image-leak-cases-karnataka-police/articleshow/131805260.cms.> accessed 13 June 2026

35. Law Journals, "Deepfakes and Emerging Challenges to Privacy and Criminal Law", Vol. 12, Issue 1(2026), https://www.lawjournals.org/assets/archives/2026/vol12issue1/12074.pdf.

36. Indian Journal of Law and Legal Research, "Section 78 BNS: Cyberstalking, Gender and Digital Evidence in Contemporary India",https://www.ijllr.com/post/section-78-bns-cyberstalking-gender-and-digital-evidence-in-contemporary-india.

37. Deepfake Regulation vs Free Speech: Should India Criminalise AI-Generated Deepfakes Under Fundamental Rights Concerns? LawVS,

38. https://lawvs.com/articles/deepfake-regulation-vs-free-speech-should-india-criminalize-ai-generated-deepfakes-under-fundamental-rights-concerns>accessed 13 June 2026

39. The Face of Fraud: A Comparative Analysis of Deepfake Regulations in the EU AI Act v India's IT Rules, IJIRT(2026), https://ijirt.org/publishedpaper/IJIRT191410_PAPER.pdf.> 13 June 2026

40. Deepfake Injunctions India, Global Law Experts, https://globallawexperts.com/deepfake-injunctions-india/ >accessed 14 June 2025

41. Is the Indian Law Equipped Enough to Deal with Deepfakes?, iPleaders https://blog.ipleaders.in/is-the-indian-law-equipped-enough-to-deal-with-deepfakes/ >accessed 14 June 2026

42. Regulating Deepfake Technology: Ethical and Legal Challenges under Indian Law, Parujanwala Law Academy, available at:https://www.pahujalawacademy.com/regulating-deepfake-technology-ethical-and-legal-challenges-under-indian-law >accessed 15 June 2025

43. IT Rules 2026: Deepfake Takedown, 3 Hour Rate and AI Labelling Explained, LawSikho, available at: https://lawsikho.com/blog/it-rules-2026-deepfake-takedown-3-hour-rule-and-ai-labelling-explained/ >accessed 15 June 2026

44. The Indian Law Equipped Enough to Deal with Deepfakes ?, iPleaders, https://blog.ipleaders.in/is-the-indian-law-equipped-enough-to-deal-with-deepfakes/.>accessed 15 June 2026

45. Regulating Deepfake Technology: Ethical and Legal Challenges under Indian Law, Parujanwala Law Academy.https://www.pahujalawacademy.com/regulating-deepfake-technology-ethical-and-legal-challenges-under-indian-law.>accessed 15 June 2026