

Deepfakes and the Law in India: Copyright, Personality Rights and the Need for a Comprehensive Legal Framework

Rakesh Kumar*

Amity Law School, Amity University, Patna.

ABSTRACT

The fast growth of artificial intelligence has enabled the creation of deepfakes, which are very realistic audio, video, and images that are made or changed using artificial means. Even though deepfakes can be useful for art, jokes, teaching, and fun, they are now more often used to pretend to be someone else, share fake news, harm people's reputations, steal money, and create unwanted explicit photos or videos without consent. These uses put a person's privacy, dignity, identity, and ability to control their own creative work at risk. This paper looks at how Indian laws deal with deepfakes right now. It looks at the Information Technology Act from 2000, the Bharatiya Nyaya Sanhita from 2023, the Information Technology Rules from 2021 which were updated in February 2026, and the Copyright Act from 1957. It also looks at personality rights and the right of publicity. It also looks at the techniques used to find deepfakes and the challenges of proving who made them, determining responsibility, and helping victims get help quickly. The paper says that the current rules, even though they work to some extent, are broken up into different parts, weren't made with synthetic media in mind, and only give some protection to a person's digital image. Victims continue to have difficulty getting help that comes quickly and really makes a difference. India needs a clear and full plan that brings together changes in laws, better technology, and working with other countries. This plan should balance new ideas and free speech with making sure people's rights are protected.

Keywords: Deepfakes, Artificial Intelligence and Law, Privacy Rights, Personality Rights, Copyright Law, Right of Publicity, Defamation, Deepfake Detection, Regulatory Framework in India

INTRODUCTION

Artificial Intelligence (AI) is among the most consequential technological changes of the twenty-first century, and deepfake technology is one of its most striking and controversial products [1]. Deepfakes are synthetic media produced by AI systems trained on large quantities of real content. Having studied how a person looks, moves and sounds, these systems can generate videos, audio recordings and photographs that appear authentic even though the events they depict never took place. The same technology that allows filmmakers to de-age actors, teachers to build engaging lessons and doctors to detect tumours more accurately is now being used, with growing frequency, to spread falsehoods, injure reputations, steal identities and create harmful sexual content without the consent of the person shown.

The danger of deepfakes lies partly in the way people process information. Human beings tend to trust what

they see and hear, and for most of the history of recorded media, a video or a voice recording was treated as reliable evidence that something had happened. Deepfakes weaken that assumption. When a convincing fabrication can be produced on a mobile phone within minutes, it becomes increasingly difficult for an ordinary viewer to separate the genuine from the manipulated. The consequences are not shared equally. Studies and reported incidents consistently show that women have been affected more severely than others, particularly through the non-consensual use of their faces in explicit material [1], [3].

The harms of deepfakes cut across several areas of law at the same time. They infringe personality rights, which protect a person's name, image, voice and overall identity, by creating false endorsements and by damaging a person's standing in society. They invade privacy by creating and circulating false and

Relevant conflicts of interest/financial disclosures: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.



unwanted content about a person without permission, a concern that gains weight from the recognition of privacy as a fundamental right under Article 21 of the Constitution in *Justice K.S. Puttaswamy v. Union of India* (2017). At the same time, deepfakes built from copyrighted photographs, films, songs or performances may amount to unauthorised copying, adaptation and communication to the public, which affects the rights of creators, performers and other copyright owners [2].

Existing laws were not drafted to deal with manipulation of this kind. Their application differs from one situation to another, and the law must keep pace with technology that changes every few months. India still has no dedicated statute that protects the personality rights of performers and other individuals. Courts have therefore developed protection case by case, and Indian High Courts have granted injunctions to well-known personalities such as Amitabh Bachchan (2022) and Anil Kapoor (2023) against the unauthorised commercial use of their names, images and voices. For ordinary citizens, who cannot easily approach a High Court for a personality-rights injunction, copyright law and the general provisions of the criminal and technology statutes remain the primary avenues of redress.

This paper examines the legal issues raised by deepfakes, with particular attention to their relationship with copyright and with the original works on which they are based. It asks two questions. First, what are deepfakes, and how do they relate to copyright concerns? Second, what legal options are available to creators and to individuals who are targeted by deepfakes? The study adopts a doctrinal and analytical approach and draws on academic articles, journals, statutes, government press releases and online sources. It assesses how far existing copyright rules and the wider legal framework can regulate deepfake technology, and it identifies the areas in which stronger protection is urgently needed.

The paper is organised as follows. Part II explains the meaning, technology and origins of deepfakes, together with the difficulty of defining them. Part III reviews the technical methods used to detect deepfakes and their limitations. Part IV analyses the statutory provisions, regulatory measures and institutional mechanisms available in India. Part V concludes and offers suggestions for reform.

II. THE CONCEPTUAL FOUNDATION: WHAT IS A DEEPFAKE?

(A) Meaning, Technology and Origins

A deepfake is a piece of synthetic media, whether a picture, a video or a sound recording, that has been created or altered by artificial intelligence so that it appears to show a real person doing or saying something that the person never actually did [4], [5]. The word combines "deep learning" and "fake", and it describes both the underlying technology and the content that technology produces. The term became widely known in late 2017, when a Reddit account named "deepfakes" posted videos in which the faces of celebrities had been swapped onto other bodies using AI. The availability of open-source code and simple mobile applications then allowed the technique to spread rapidly into politics, business, the military and popular culture [5].

Most deepfakes are created with Generative Adversarial Networks (GANs) [6], [7]. A GAN has two parts that work against each other. One neural network, called the generator, produces the fake content. A second network, called the discriminator, examines that content and judges whether it looks genuine. Each round of feedback forces the generator to improve, so the fabricated output becomes steadily more realistic. By studying large quantities of data, these systems learn a person's face, expressions, mannerisms and voice. They can then replace one person with another or generate entirely new material that never existed. The results are often very hard to distinguish from authentic recordings [7], [8].

Two features of this process matter for the law. The first is the scale of data involved. Training a convincing model normally requires many images, video clips or voice samples of the target, and those inputs are frequently taken from copyrighted films, photographs, songs or social media accounts without the knowledge of the owner. The question of whether the use of protected material to train such a system is itself lawful has been raised in international discussion, including in a draft issues paper on intellectual property and artificial intelligence prepared by the World Intellectual Property Organisation (WIPO) in December 2019 [1]. The second feature is the falling cost of production. What once required a studio and specialist skills can now be done by an individual with

free software, so the number of potential wrongdoers is very large and difficult to trace.

(B) Legitimate Uses and Harmful Misuse

Deepfakes are not harmful by nature. They are used in entertainment, education, gaming and voice-based customer services. In films, they offer a less expensive alternative to elaborate visual effects or reshooting scenes, for instance, when actors are made to look younger or when performers who have died, such as James Dean, are brought back to the screen. In education, synthetic video can allow a historical figure to "speak" in a classroom or allow a lecture to be delivered in several languages. In medicine, synthetic images are used to train diagnostic systems when real patient data is scarce or confidential.

Indian examples show the same range of uses. The Cadbury advertisement featuring Shah Rukh Khan and the Hrithik Roshan Rakhi campaign allowed members of the public to place themselves in the advertisement by uploading their own photographs, and in both cases the use was authorised and commercial [1]. These examples show that the technology can be lawful when the consent of the person whose likeness is used has been obtained.

The same technology is also used to create non-consensual pornography of celebrities and private individuals, and the multilingual video of the politician Manoj Tiwari, circulated during the Delhi elections, shows how it can be used in political communication [1]. In that instance, the purpose of the video was campaigning, but it demonstrated how easily a leader can be made to address voters in a language he does not speak, and how the same method could be used to put false and inflammatory words in his mouth. The greatest risk is the production of false information that appears to come from trusted sources, such as a public official, a news anchor, a company executive or a family member. Deepfakes also violate privacy rights and appropriate the intellectual property of others [1].

Voice cloning deserves separate mention. Audio deepfakes need only a short sample of speech and can be used in telephone scams in which a victim is persuaded that a relative or a senior officer of a company is asking for urgent money. Because there is no visual element to examine, audio fakes are in some ways harder for victims to question. This is one reason why India's detection efforts, discussed in Part IV, include

a system specifically for real-time voice deepfake detection [11].

(C) The Difficulty of Defining Deepfakes

Defining deepfakes is not a simple exercise. There is no single, universally accepted definition, and it is hard to draw a line between a deepfake and an ordinary edited or fake video. Detection methods frequently work on both kinds of content. Some scholars use the word "deep" to describe any sophisticated technique and not only deep learning, and they distinguish deepfakes from "shallowfakes" and "cheapfakes", which are made with conventional editing tools such as slowing down a clip or changing its caption. Another expression, "deep synthesis", which appears in Chinese regulation, has not become common in other jurisdictions [7].

The lack of a settled definition has practical effects. A law that is drafted too narrowly, for example by referring only to GANs, will be outdated as soon as a new generation technique appears. A law drafted too widely may catch harmless editing, parody and ordinary photo filters. India's amended IT Rules approach the problem by regulating "synthetically generated information" in general rather than a particular technique, which is a more technology-neutral approach [11]. However, the absence of a clear statutory definition that applies across the IT Act, the criminal law and the Copyright Act continues to cause uncertainty for courts, platforms and victims.

III. CHALLENGES IN DETECTING AND ADDRESSING DEEPFAKES

(A) Detection Methodologies and Frameworks

The continuing contest between tools that create deepfakes, such as those based on GANs and autoencoders, and systems that try to detect them exposes a serious weakness in today's digital media. Early detection models relied on simple classifiers and manually designed features to identify unusual eye blinking, irregular head movements or facial inconsistencies. These methods did not perform well when they were applied to varied, real-world data sets, because they had been tuned to the particular artefacts of a particular generation method.

Newer content-generation methods now make it easier to swap faces, synchronise lips with spoken words, and alter audio and video in ways that look highly

realistic. As a result, security and trust in the online world face greater risks than ever before. Modern studies therefore stress the use of organised, step-by-step processes, such as the Cross-Industry Standard Process for Data Mining (CRISP-DM), to plan, carry out and improve data analysis and model-training projects in a clear and effective manner [9], [10]. CRISP-DM moves a project through business understanding, data understanding, data preparation, modelling, evaluation and deployment, and it allows a team to return to earlier stages when the results are not satisfactory. For deepfake detection, this means that the choice of data, the preparation of video frames and the evaluation of the model are treated as deliberate stages and not as afterthoughts.

(B) Technological Advancements and Hybrid Architectures

To overcome the limits of relying on a single model, modern systems combine different learning approaches. This helps them understand both spatial differences within an image and changes that occur over time. Convolutional Neural Networks (CNNs) examine the pixels of each frame to find fine details and defects such as visual glitches, blending errors and traces of image transformation. Because a video unfolds over time, Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) networks are used to understand how movement and expression change from one frame to the next, so that unnatural transitions can be identified [9], [10].

Transformer models and Fourier Transform-based analysis have also been applied to capture long-range relationships in the data and the small errors that remain after the synthesis process. Frequency analysis is useful because generation methods often leave faint, regular patterns in the frequency components of an image that the human eye cannot see. By combining spatial, temporal and frequency information in a single pipeline, detection systems achieve noticeably better accuracy and more balanced results when they are tested on standard benchmark collections such as FaceForensics++ [9], [10].

(C) Best Possible Outcome and Future Scope

Despite this progress, robust deepfake detection must still overcome several important research problems. Detectors must adapt to new real-world data that they have not seen before, because a model trained on one

benchmark often performs worse on videos that have been compressed, resized or re-uploaded on social media. They must manage high computational demands, which matters most when a platform has to scan very large volumes of content. And they must remain effective against adversarial attacks, in which a creator deliberately modifies a fake to fool the detector [10].

The most promising way forward is to build systems that can detect fakes in real time by examining several types of information together: what a person is seeing, how a person is behaving, including facial expressions and lip movements, and what a person is hearing. If such hybrid AI models are used together with automated data-preparation tools and sustained efforts to teach the public about media, security systems can limit the spread of false information, protect democratic discussion and restore trust in digital media [10]. Detection technology, however, can never be a complete answer by itself. Because detectors and generators improve in response to each other, legal responsibility, platform obligations and public awareness must work alongside technical tools.

IV. CORE LEGAL REMEDIES AND GOVERNMENT REGULATION

The Indian government has made significant changes to its rules and regulations in response to the growing danger of AI-generated deepfakes and synthetically generated information. The framework aims to build a safe, trusted and responsible online environment. It consists of principal statutes, revised digital rules, enforceable compliance obligations and locally developed detection technology [11]. The sections below examine each element in turn.

(A) Statutory Laws and Penal Provisions

No Indian statute uses the word "deepfake" as the name of an offence. Victims and prosecutors therefore rely on general provisions that were written for impersonation, fraud, obscenity and defamation, and apply them to synthetic media.

- **The Information Technology Act, 2000 (IT Act):** This Act prescribes punishment for computer-related offences. Section 66C deals with identity theft, which covers the fraudulent use of another person's unique identifying features, and Section 66D deals with cheating by personation

through a computer resource. Section 66E punishes the violation of privacy by capturing, publishing or transmitting images of the private area of a person without consent. Sections 67 and 67A punish the publication or transmission of obscene and sexually explicit material in electronic form, and are the provisions most often used against non-consensual explicit deepfakes. The Act also gives the government the power to issue blocking orders under Section 69A, and it provides in Section 79 that an intermediary is protected from liability for third-party content only if it observes due diligence and removes unlawful content on receiving notice or an order.

- **The Bharatiya Nyaya Sanhita, 2023 (BNS):** The BNS, which has replaced the Indian Penal Code, punishes cheating by personation under Section 319, which applies when a person cheats by pretending to be someone else. Section 336 punishes forgery, including the creation of false electronic records for the purpose of harming a person's reputation. Section 353 punishes the making and circulation of false information, statements or rumours that are likely to cause public disturbance or mischief. Where deepfakes are used by organised criminal groups, for instance in large-scale financial fraud, the provisions on organised crime in Section 111 may apply. Depending on the facts, the general provisions on defamation and on voyeurism and the insulting of the modesty of women may also be relevant.

These provisions give prosecutors a workable set of tools, but their limits are plain. Each was drafted for a different harm, so none of them captures the combined wrong of a deepfake: that a real person's identity has been taken, falsified and circulated at scale. Proving the necessary mental element, such as dishonest intention to cheat, can be difficult when the creator is anonymous or located abroad, and criminal prosecution does not by itself give the victim what is most urgently needed, which is the quick removal of the content.

(B) Copyright Law, Personality Rights and Privacy

Copyright law is the area of law that most directly addresses the creative inputs and outputs of deepfakes. Under the Copyright Act, 1957, the owner of a protected work has the exclusive right to reproduce it,

to adapt it and to communicate it to the public. A deepfake that is built from a film, a photograph or a sound recording, and that is then circulated, may amount to unauthorised reproduction and distribution, and the use of characters or performances taken from an original work without permission may infringe the owner's rights [1]. Where the deepfake is used commercially, the person who made it profits while the original author is neither credited nor paid [1].

The Act also recognises the moral rights of authors in Section 57, including the right to claim authorship and the right to restrain or claim damages for any distortion, mutilation or modification of the work that would be prejudicial to the author's honour or reputation. India is a member of the Berne Convention, and the rule that an author may object to distortion of a work that harms his honour or reputation is reflected in the Convention's provisions on moral rights [1]. Performers are protected by Sections 38 and 38A, which give them exclusive rights over their performances, and by Section 38B, which gives performers moral rights of attribution and a right to object to distortion or mutilation of the performance. These provisions are significant for actors, singers and other performers whose voices and screen appearances are copied by deepfake tools.

The Act also contains exceptions. Section 52 permits fair dealing for purposes such as criticism, review, reporting of current events and private use, and a deepfake used for parody or political satire may invoke these exceptions. The result is a balance that courts must strike case by case, because the same technique may be an infringement in one setting and a defensible comment in another.

Copyright, however, protects works and performances, not a person's face, voice or identity as such. A deepfake that uses a few seconds of an individual's publicly posted video may not infringe any copyright that the individual owns, and the individual may not be the owner of the footage in the first place. Authorship of the deepfake itself is also unsettled. The Copyright Act treats the person who causes a computer-generated work to be created as its author, but questions of originality, attribution and ownership become difficult when a model generates content autonomously or semi-autonomously [3]. The existing law may therefore leave both the person depicted and the original creator with incomplete protection,

which scholars have identified as a gap requiring legislative attention [1], [3].

Because of this gap, personality rights have become the principal civil remedy. These rights, sometimes described as the right of publicity, protect a person's name, image, voice, signature and other distinctive attributes against unauthorised commercial exploitation and misrepresentation. In India, they have been developed by courts under the law of passing off, the right to privacy and the right to dignity, and not by a specific statute. In cases such as those brought by Amitabh Bachchan and Anil Kapoor, the Delhi High Court has restrained unauthorised use of the personalities' names, voices and likenesses, including by means of AI-based tools. This approach offers fast and effective relief to the famous, but it depends on the willingness of a litigant to go to court and on judge-made principles that have not been codified. It leaves ordinary individuals, and especially women who are targeted with explicit deepfakes, with fewer practical options.

Privacy law also has a role. The Digital Personal Data Protection Act, 2023 regulates the processing of digital personal data and requires, as a general rule, that data be processed with the consent of the person concerned or for a lawful purpose. A person's facial image and voice are personal data when they identify that person, so the creation of a deepfake from such data may raise questions of consent and lawful processing. The practical enforcement of this regime against anonymous individual creators is uncertain, but it provides an additional legal basis for holding organisations that handle biometric or image data to account.

(C) IT Rules, 2021 and Recent Amendments

The most direct regulatory response to deepfakes has come through amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. The amendments notified on 10 February 2026 address "synthetically generated information", a term that covers deepfakes and other AI-created content [11]. They place the main practical obligations on intermediaries, which are the platforms through which such content is distributed.

- **Improved checks and obligations:** Intermediaries are required to take steps to prevent users from creating or sharing synthetic content that is unlawful, misleading or impersonating. Platforms

must use automated and other suitable tools to stop synthetic content that violates the law. Significant social media intermediaries, which are those with 50 lakh (five million) or more registered users in India, must make reasonable efforts to use automated tools to identify content that depicts rape or child sexual abuse and content that is identical to material that has already been removed. They must also publish compliance reports, appoint officers in India and maintain a physical address in the country [11].

- **Strict time limits for removing harmful content:** After the amendments of 10 February 2026, the time allowed for taking down unlawful information on the basis of a reasoned government intimation or a court order was reduced from 36 hours to only 3 hours. The time for resolving user grievances was cut from 72 hours to 36 hours, and for sensitive matters such as nudity and impersonation, the period was cut from 24 hours to just 2 hours. An intermediary that does not comply loses the protection of Section 79 of the IT Act, and may become liable to action or prosecution for the third-party content [11].
- **Labelling and metadata:** Platforms must ensure that permissible AI-generated content is clearly labelled and carries traceable metadata, so that users can identify it as synthetic and are not misled. Users must also be made aware of the legal consequences of creating or sharing unlawful synthetic content [11].

The shortening of the removal periods recognises something that is central to the experience of victims, which is that the harm of a deepfake grows with every hour that it remains online. A video that is shared thousands of times within a day cannot be fully recalled later, so rapid removal is often more valuable to the victim than eventual punishment of the offender. At the same time, very short deadlines put pressure on platforms to remove content first and examine it later, and this creates a real risk that lawful speech, such as satire, political criticism or journalism, will be removed by mistake. The rules include internal appeals and a requirement of a fair hearing before certain action is taken on the platform's own initiative, but the balance between speed and accuracy will have to be watched closely in practice [11]. The government has also issued advisories, including one

dated 16 March 2026 on abusive or misleading synthetic content, and has released a standard operating procedure for non-consensual intimate imagery on 11 November 2025 to guide victims, intermediaries and law enforcement [11].

(D) AI Governance and Indigenous Detection

The India AI Governance Guidelines, released on 5 November 2025, set out a risk-based and proportionate framework for the safe, trusted and responsible development and use of AI [11]. The guidelines favour measured regulation that addresses identifiable harms and avoids discouraging innovation, which is consistent with the stated aim of the IndiaAI Mission.

Under the Safe and Trusted AI pillar of the IndiaAI Mission, projects for detection technology developed in India have been approved in educational institutions [11]. These include Saakshya, a multi-agent deepfake detection framework developed by IIT Jodhpur and IIT Madras; AI Vishleshak, which improves the detection of audio and visual forgeries; and a Real-Time Voice Deepfake Detection System developed at IIT Kharagpur. The Indian Computer Emergency Response Team (CERT-In) has also published an advisory on deepfake threats, issued in November 2024 [11]. Developing such tools within the country is significant because detection systems trained on foreign data may not work as well on Indian faces, languages and accents. The public material on these tools does not report their accuracy figures, so their real-world performance remains to be assessed independently.

(E) Implementation, Redressal and Reporting

A person who is dissatisfied with the way a platform has dealt with a complaint can appeal online to the Grievance Appellate Committee (GAC), the central-level appellate forum for challenging the content-moderation decisions of intermediaries, through its website gac.gov.in. This provides a route that does not require the cost and delay of a court case [11].

Cybercrimes, including deepfakes, can be reported through the National Cyber Crime Reporting Portal (cybercrime.gov.in), which gives particular attention to crimes against women and children, or by calling the helpline number 1930. The portal accepts reports of deepfakes, financial frauds and misuse of content. The SAHYOG Portal, managed by the Indian Cyber Crime Coordination Centre (I4C), enables automated

and centralised removal notices to be sent to intermediaries by the appropriate governments and their authorised agencies. The Samanvaya Platform provides analytics-based linking of criminals and crimes across states, and its Pratibimb module maps criminal locations and crime infrastructure. The Press Information Bureau reports that Samanvaya has so far supported the arrest of 12,987 accused, the identification of 1,51,984 criminal linkages and 70,584 requests for cyber investigation assistance [11].

These institutions show that India has built considerable machinery for responding to cybercrime. Their effectiveness for deepfake victims depends on awareness, because many people, particularly those in smaller towns, do not know that these channels exist. It also depends on the ability of police and prosecutors to preserve electronic evidence and trace anonymous accounts across platforms and borders, an area in which capacity remains uneven.

V. CONCLUSION AND SUGGESTIONS

CONCLUSION

Deepfakes, which are usually made using Generative Adversarial Networks (GANs), show both the beneficial and the harmful sides of artificial intelligence. They are used in film, advertising and education, but they can also be used to spread false information, impersonate others, commit financial fraud, harm reputations and distribute explicit content without consent. This paper has explained that a single deepfake can affect privacy, personal rights and copyright at the same time, and that the harm to a victim is often immediate and difficult to reverse.

Detection is difficult. Tools based on CNNs, LSTMs and frequency analysis perform well on benchmark tests such as FaceForensics++, but they often perform less well on new, compressed, real-world content, and those who make such content keep improving their methods. As for the law, India relies on the IT Act, 2000, which includes Sections 66C, 66D, 66E, 67, 67A, 69A and 79, on the Bharatiya Nyaya Sanhita, 2023, which covers Sections 111, 319, 336 and 353, and on copyright law. In February 2026 the IT Rules were amended so that content that violates the rules must be removed within 3 hours of a valid order or intimation, and permissible AI-generated content must be clearly labelled and carry traceable metadata. Platforms that fail to comply lose protection from

legal liability under Section 79. Indigenous tools such as Saakshya and AI Vishleshak are also positive steps. Even so, these rules are scattered, were not designed specifically for deepfakes, and usually operate after the damage has been done. Copyright law helps when someone copies protected works, but it does not fully protect a person's face, voice or identity. Personality rights, which fill part of the gap, have so far been developed by courts without a statute. What is needed is not another isolated advisory but a connected framework in which law, technology and institutions support one another.

(B) Suggestions

1. **Enact a dedicated law.** The law should clearly define deepfakes and synthetic media, and should distinguish between their harmful uses and legitimate ones such as satire, art, journalism and education. A technology-neutral definition will remain useful as new methods of generation appear, and a clear definition will reduce uncertainty for courts, platforms and victims.
2. **Protect personality rights by statute.** The use of a person's name, image or voice without permission should be made unlawful, and the person should have a right to compensation. Codification would make these protections available to ordinary individuals and not only to celebrities who can afford to litigate, and would give courts consistent standards in place of case-by-case development.
3. **Amend the Copyright Act.** The Act needs to clarify who owns work created by AI, the rights of performers, and who is responsible when unauthorised fake videos or images are made. It should also address whether the use of copyrighted material to train generative models requires the permission of the owner, and should preserve sensible exceptions for criticism, parody and research.
4. **Strengthen detection and forensic capacity.** The government should continue to support indigenous detection research under the IndiaAI Mission, require independent testing of such tools on realistic and compressed Indian-language data, and train police, prosecutors and judges in the handling of digital evidence so that a genuine recording can be distinguished from a fabricated one in court.
5. **Make platforms accountable.** Platforms should be required to label synthetic content, attach traceable metadata and act quickly on complaints. Safeguards must also be built in so that content that is lawful is not removed by mistake, including notice to the uploader, a fair hearing and an effective appeal, so that speed does not come at the cost of free expression.
6. **Support victims.** Reporting through the National Cyber Crime Portal, the helpline number 1930 and the Grievance Appellate Committee should be made simple and easy to use. Victims, especially women, should receive quick help and support, including legal aid, counselling and assistance in having content removed from every platform on which it appears.
7. **Increase public awareness.** Students, teachers and the general public should be taught to recognise false information and to know where to report it. Education from school level onward, together with a habit of verifying content before forwarding it, can reduce the circulation of deepfakes at the source [1].
8. **Cooperate internationally.** Deepfakes can spread across countries, so India should work with other nations to share information, to agree on common standards for labelling and detection, and to make it easier to trace and act against offenders located abroad.

India needs strong laws, dependable technology, speedy justice and informed citizens working together. Only through such coordination can people's dignity and rights be kept safe while allowing AI to develop in a beneficial and responsible way.

REFERENCES

1. "A Study on Deepfakes and Copyright Infringement," *International Journal of Law Management & Humanities (IJLMH)*. Available:

1. <https://ijlmh.com/wp-content/uploads/A-Study-on-Deepfakes-and-Copyright-Infringement.pdf>
2. E-Journal of Academic Innovation and Research in Intellectual Property Assets (E-JAIRIPA), Vol. V, Issue I, January–June 2024, pp. 1–13.
3. "Understanding Deepfake Technology in the Aspect of Copyright Law," Indian Journal of Legal Law and Research (IJLLR). Available: <https://www.ijllr.com/post/understanding-deepfake-technology-in-the-aspect-of-copyright-law>
4. ACM Digital Library, "Deepfake," 2023. Available: <https://dl.acm.org/doi/10.1145/3603781.3603790>
5. TechTarget, "Deepfake," WhatIs.com. Available: <https://www.techtarget.com/whatis/definition/deepfake>
6. G. Bharathi Mohan et al., "An analysis of large language models: their impact and potential applications."
7. M. T. Irfan, "On Machine Learning and Deep Learning based Deepfake Generation and Detection," Indian Journal of Law and Legal Research, vol. VIII, issue I, ISSN 2582-8878.
8. PubMed Central, article PMC11408348. Available: <https://pmc.ncbi.nlm.nih.gov/articles/PMC11408348/>
9. International Journal of Creative Research Thoughts (IJCRT), paper IJCRT2605432. Available: <https://ijcrt.org/papers/IJCRT2605432.pdf>
10. M. S. Raghava, S. P. Tejashwini, Kavya Sree, A. Sneha and R. Naveen, "AI Deepfake Detection," Dept. of Artificial Intelligence and Machine Learning, Dayananda Sagar Academy of Technology and Management, International Journal of Novel Research and Development (IJNRD), paper IJNRD2310407. Available: <https://www.ijnrd.org/papers/IJNRD2310407.pdf>
11. Press Information Bureau, Government of India, Press Release PRID 2295500. Available: <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2295500&=1&lang=1>

HOW TO CITE: Rakesh Kumar, Deepfakes and the Law in India: Copyright, Personality Rights and the Need for a Comprehensive Legal Framework, *Int. J. Sci. R. Tech.*, 2026, 3 (10), 1250-1258. <https://doi.org/10.5281/zenodo.23662321>