



International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Borrowed Faces, Fabricated Voices and Legal Challenges of Deepfakes

Nitish Kumar Nigam,¹ Ansh Singhal,² Sanidhya S. S. Chauhan³

¹ Vth Year, B.Sc.LL.B. (Hons.) [Cybersecurity], National Law Institute University, Bhopal.

² Vth Year, B.A.LL.B. (Hons.) [Cybersecurity], National Law Institute University, Bhopal.

³ Vth Year, B.Sc.LL.B. (Hons.) [Cybersecurity], National Law Institute University, Bhopal.

ABSTRACT :

With all the attention and excitement over Generative Adversarial Networks (GANs), diffusion models and the like, deepfakes have moved on from a technological curio to something of major legal social and ethical concern across the globe. The article first surveys the international legal and regulatory response to those issues before tracing, on Indian law, two concurrent processes: slow-burning legislative and executive regulation at the national level culminating in 2026 Amendment to the Intermediary Rules; and a faster pace of development of judicial pronouncements over IP/personality-fears with High Courts extending copyright. Trade mark and privacy principles, by way of illustrations by case studies of which in broad strokes there are two, the Delhi high courts (Grok etc. and Chaitanya Rohilla) and Bombay high court (Rashmika) and in part Delhi as well the Bollywood 'star', including as a particular case study an analysis of the case of Getty Images v Stability AI, on training data and IPR for AI. The article then explains two paths of development of Indian law with regard to deep-fakes; it also makes a prediction that neither the 2026 Rules, albeit a move from warnings to statutory rule, would be sufficient to deal with the issue.

Some such cases could be use of AI to impersonate celebrities (e.g. Anil Kapoor), the recent 'Rashmika Mandanna' issue and subsequent regulatory action. This could be contrasted with Chaitanya Rohilla PIL and more generally with cross border issues such as the recent expanding 'Grok/xAI' litigation over various jurisdictions. Although the 2026 Rules are important step from soft advisories to hard law, they still cannot handle the depth of the issue and we are missing a number of essential aspects like a persona right and commensurate criminal offences; as well as a serious and credible mechanism for compensating victims.

Introduction

What if one day you woke up, and there was a video of yourself all over the internet? The face is your own, the voice sounds like yours and even the way you move looks familiar. But you did not say or do what the video depicts. The video has already circulated widely, reaching thousands of people with the damage this dissemination may have caused being hard to fix even after repeating that it is fake. Though it sounds like a far-fetched possibility, that has become an ever-more-real worry especially for women and youth who are constantly bombarded with manipulated, non-consensual photos. This technology is referred to as “deepfake”. Deepfakes are synthetic media that have been created using artificial intelligence to manipulate or generate images, videos, audio or other digital content where an existing person is made to appear like someone who never said what they did.

AI systems are already able to accurately recreate a person's facial features, voice, gestures and mannerisms with publicly available photographs images/videos/audios recording. While the technology itself is largely benign, when applied to things other than entertainment, education and production of content for accessibility purposes. And yet its potential abuse raises significant legal and ethical issues. Deepfake is used for impersonation, fraud and misinformation as well as harassment, distribution of non-consensual sexual content or the unauthorised use of a person's information against their will. This availability of deepfake content creates a specific challenge in that such videos can respond to trends and go viral much faster than any effective remedy on the legal scale.

The old aphorism that “the camera never lies” once embodied a rudimentary premise about the truthfulness of audio-visual recordings. That assumption was all but impossible to uphold by 2026. Researchers have been training artificial intelligence (AI) to create hyper-realistic images, video + audio and other synthetic data that can mirror real people/experiences/interactions. The evolution of this process has transformed deepfakes from a scientific novelty or digital weapon for spreading fake news on social networks into one of the most pressing legal, societal and ethical issues. The rise of generative AI has made the line between real and fake content very much gray.

A person's face can be superimposed onto another individual, their voice can be cloned, and entirely fabricated events can be presented as genuine. Synthetic data can similarly reproduce or simulate information that appears real while having no corresponding real-world event or source. This creates

difficult questions surrounding consent, privacy, intellectual property, personality rights, misinformation, fraud and accountability. The challenge is therefore no longer simply identifying whether a particular piece of content is “fake”, but determining who should be responsible when synthetic content causes real-world harm. As deepfake and synthetic-media technologies continue to advance, existing legal frameworks must confront the growing difficulty of protecting individual rights and maintaining trust in an increasingly artificial digital environment.

Understanding Deepfake and Synthetic Media

Recent practical advancements in Artificial Intelligence (AI) have had a significant impact on a range of fields, including digital media in general, with serious repercussions. AI is seen as a paradigm-changing technology due to the numerous practical applications that have been demonstrated in recent years, the majority of which are credited to a subfield of AI known as “Deep Learning”.¹

Deepfake AI technology works through a series of steps to create realistic fake videos or audio of people:

- It starts with **data collection** which involves gathering multiple films, photos, and audio recordings of an individual. This data is utilised to assist the AI understand how the individual appears and sounds.
- The training stage “During this phase, the AI also learn how to generate fake content in terms of Generative Adversarial Networks (GANs). The generative tries to produces a dummy image or video, and then the descriptive checks if it’s either real or fake. The exchange process enables the generative to progressively produce more believable content by perfecting its images.
- Now that, AI can also synthesize deepfakes “Once satisfied that is capable, the AI can proceed to generate a new video or audio clip that closely replicates the persona it is supposed to mimic.
- The AI matches the movements as well as expressions of the chosen persona, with that of the intended audio or video.
- The final step is **rendering**, where the deepfake video or audio is polished to look even more realistic by fixing any small mistakes. GANs, which involve two competing AI systems, are key to this process, one creating the fake content and the other judging its quality.

A **deepfake** is a category of synthetic media , an image, audio clip or video , generated or altered using deep-learning techniques so as to depict a real, identifiable person saying or doing something they did not in fact say or do, in a manner that a reasonable viewer would take to be authentic.² It is best understood as a subset of the broader category of *synthetically generated information* (“SGI”), a term now used in Indian delegated legislation to capture any content “artificially or algorithmically created, generated, modified or altered using a computer resource, in a manner that such information reasonably appears to be authentic or true”, regardless of whether it depicts a real person or is otherwise deceptive.³

Deepfakes are the product of two categories of ML techniques (which are trained at odds with each other): machine-generated, visual-art models called Generative Adversarial Networks (GANs), where a “generator” model creates synthetic images and a “discriminator” tries to differentiate the originals from the fakes until the fakes get really good; and diffusion models (an approach most currently behind such tools as Stable Diffusion and Midjourney), which develop the ability to reconstruct an image by starting with it full of noise and gradually stripping away that noise. Some diffusion models can also clone a person’s voice if trained on a few seconds to a few minutes of it. Synthetic data, a term that is similar but not identical to synthetic-meaning “artificial”-media, are artificially generated sets of data that are useful for training and testing machine-learning systems when real-world data is in short supply, is very private or is costly to gather-for example, if we wanted to create synthetic medical images to test a diagnostic algorithm, but without seeing actual patient information. Synthetic data is, in itself, a legitimate and often privacy-protective technique; the legal and ethical difficulty in the deepfake context arises specifically where the underlying training data or the generated output involves an identifiable real person’s biometric attributes without consent, or where copyrighted material is scraped to train a generative model, as alleged (unsuccessfully, in large part) in *Getty Images v Stability AI*⁴ discussed below and other case studies.

¹ R. Chesney and D. Citron, *Deepfakes and the new disinformation war: The coming age of post-truth geopolitics*. Foreign Affairs, vol. 98, no. 1, pp. 147–153 (2019), available at < <https://perma.cc/TW6Z-Q97D>> (accessed on 29th August 2026).

² Article 3 (60), Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on Artificial Intelligence, Official Journal of the European Union, 12th July 2024, available at < https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689> (accessed on 29th August 2026).

³Ministry of Electronics and Information Technology, *Explanatory Note to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2025* (22 October 2025), para 3, available at <[official MeitY Explanatory Note](#)> (accessed on 30th August 2026).

⁴ *Getty Images (US) Inc & Ors v Stability AI Ltd*, [2025] EWHC 2863 (Ch), available at <<https://www.judiciary.uk/wp-content/uploads/2025/01/Getty-Images-and-others-v-Stability-AI-14.01.25.pdf>> (accessed on 29th August 2026).

The International Regulatory Landscape

It is clear that no jurisdiction has so far enacted a standalone 'deepfake law' and most regulatory approaches incorporate new transparency and labelling rules atop existing intermediary liability, data-protection and/or criminal-law frameworks. Four approaches merit consideration

European Union: Transparency and Labelling under the AI Act

Article 50(4) of the EU AI Act⁵ Article 50(4) of the EU AI Act states that a deployer of an AI system which creates or manipulates “image, video or audio material which is in whole or in part artificially generated or manipulated to make it appear to be original, authentic and true, shall disclose that the material has been artificially generated or manipulated”.²⁵ In keeping with its principle of trying to define the scope of the obligation as widely as possible and even if it's made in a way that does not induce deception, ²⁶ even if the material itself depicts fictitious entities, ²⁷ except where the material is “clearly artistic, creative, satirical, fictional or similar”, it must disclose the artificial or manipulated content “ in an appropriate manner which does not impede the viewing or pleasure of the work”.²⁸ Our two takeaways from the EU model are obvious. First, it puts compliance firmly on the shoulders of the deployer, or, the actual publicizing or showing of the deepfake material at the end-user level rather than only on the creator of the AI model (since that's where most of the harm happens), and second, it imposes a source labeling regulation that's in stark contrast to our intermediary due diligence model that primarily hinges on loss of safe harbour.

The transparency obligations became binding across the Union from 2 August 2026, and are backed by fines of up to €15 million or 3% of an undertaking's global annual turnover, whichever is higher.⁶ Providers of generative AI systems are separately required to embed machine-readable markers in their outputs, with the AI Office coordinating a voluntary Code of Practice on the marking and labelling of AI-generated content as a safe-harbour route to compliance.

United States: Fragmented Regulation and Emerging Liability

The United States has no comprehensive federal deepfake statute. Regulation has instead developed at state level, several states criminalise non-consensual deepfake pornography or election-related deepfakes, and Minnesota's first-in-the-nation ban on “nudification” technology took effect on 1 August 2026. At the federal level, the proposed NO FAKES Act, which would create a federal right against unauthorised digital replicas of a person's voice or likeness, remains pending. In the absence of a targeted statute, plaintiffs harmed by the Grok controversy have instead relied on tort and product-liability theories, arguing, in effect, that an image-generation feature with foreseeable, profitable potential for abuse is itself a design defect.⁷

United Kingdom: Criminal Law and Emerging Copyright Concerns

The UK's Online Safety Act 2023⁸ criminalises the distribution of “non-consensual” images involving real and sexualised deep-fake-style image manipulation” though it has yet to introduce deepfake specific transparency legislation, unlike, for instance, the EU's AI Act. Its main substantive contribution to date to deepfake law may indeed lie in the Courts – particularly in *Getty Images v Stability AI*, which dealt with whether deepfakes can constitute copyright infringement training their generative models on web-scraped image libraries.

China: Regulating Deep Synthesis through Administrative Rules

New Regulations on Online Information and Deep Synthesis, The Provisions on the Administration of Deep Synthesis of Internet-based Information Services, a joint action from China's Cyberspace Administration, the Ministry of Industry and Information Technology and the Ministry of Public Security, were implemented from January 10, 2023.⁹ These regulations mandate that “deep-synthesis” service operators (1) procure informed consent to

⁵Article 50(4), Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on Artificial Intelligence, Official Journal of the European Union, 12th July 2024, available at < https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689 > (accessed on 29th August 2026).

⁶Art. 50(1), Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down Artificial Intelligence Act, Official Journal of the European Union, available at < <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689> > (accessed on 28th August 2026).

⁷ NO FAKES Act of 2025, S. 1367, 119th Cong. (2025), introduced in the United States Senate on 9 April 2025, available at <<https://www.congress.gov/bill/119th-congress/senate-bill/1367>> (accessed on 30th August 2026).

⁸ UK Online Safety Act, 26th October 2023, available at <<https://www.legislation.gov.uk/ukpga/2023/50/2026-06-29>> (accessed on 29th August 2026).

⁹Article 12, Provisions on the Administration of Deep Synthesis of Internet-based Information Services, Order No. 12 of the Cyberspace Administration of China, Ministry of Industry and Information Technology, and Ministry of Public Security, effective 10 January 2023, available at <https://www.cac.gov.cn/2022-12/11/c_1672221949354811.htm> (accessed on 29th August 2026).

edit an individual's biometric information including their voice and face; (2) plainly mark any synthetic output or output that has been edited; (3) ensure authentic user identity through real-name registration and (4) carry out security reviews when providing designated high-risk functions. Further obligations related to content review and algorithmic transparency were superimposed on public-facing "generative AI" services by the subsequent Interim Measures for the Management of Generative AI Services, effective since August 15, 2023.¹⁰

China's is a more centralised, upfront framework than either the EU's deployer-centred transparency approach or India's intermediary liability framework. However, its implementation and mechanics around "consent-before-synthesis" and real-name verification provide informative comparison as these become elements under consideration by Indian policymakers.

The Indian Standpoint

India's legal response to deepfakes has developed on two parallel tracks. The first is the executive and legislative approach, which has progressed relatively slowly and eventually led to the 2026 amendment to the Intermediary Guidelines. The second is the judicial approach, which has moved more quickly, with the Delhi and Bombay High Courts using existing principles of copyright, trade mark and constitutional privacy law to provide remedies for violations of personality rights. The discussion below examines both approaches, followed by the key criminal-law provisions that are commonly used in individual deepfake cases.

Information Technology Act, 2000: Existing legal Remedies

There is nothing in the IT Act that explicitly refers to "deepfake" or "synthetic media", and instead most cases relating to them are charged under the generally-applicable cyber-offence provisions of the Act. Section 66C addresses identity theft – deception or fraudulent or dishonest use of another's e-signature, password, or any other unique identification feature, while Section 66D addresses cheating through personation by means of a computer resource. Section 66E addressed capture, publication or transmission of images in private area in certain circumstances involving violation of privacy. Section 67(1) and 67A (1) deal with publishing or transmitting or causing to be published or transmitted (as applicable) obscene and sexually explicit content respectively.¹¹

There is section 79 which gives safe harbour in qualified form to intermediaries for user content provided that the intermediaries exercise due diligence and abide by directions of government and court taking down requests, this section is underpinning what the 2021/2026 Intermediary Guidelines regime is.¹²

The Intermediary Guidelines and Digital Media Ethics Code Rules: from 2021 to the 2026 Amendment

However, the original 2021 Rules did not contain the definition of or targets for "synthetic content", though these general "due-diligence" requirements were already placed upon intermediaries. The now-famous Rashmika Mandanna controversy and a string of pre-poll deepfakes propelled MeitY into action with advisory notices issued to Significant Social Media Intermediaries ("SSMIs") late in 2023, directing them to label, "misinformation and deepfakes" within specific timeframes.¹³ As these notices are non-binding in nature, it was insufficient, prompting MeitY to issue the Draft Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules 2025 on 22 Oct 2025, for public comment which, for the first time, contained the statutory category of "synthetically generated information".¹⁴ After public consultations, which the Internet Freedom Foundation contended treated "virtually all synthetically generated content as suspect", potentially creating a system which will do the same job in the capacity of a tool of censorship as it set out to target a narrow range of real harms caused by deepfakes.¹⁵ the Central Government notified the final Information

¹⁰Arts. 9, 14-17, Cyberspace Administration of China, *Provisions on the Administration of Deep Synthesis of Internet-based Information Services*, Order No. 12, effective 10 January 2023, available at <[Cyberspace Administration of China \(official text\)](#)> (accessed on 29th August 2026).

¹¹ Sec 66C–66E, 67, 67A and 79, Information Technology Act, 2000, available at <[India Code – Information Technology Act, 2000](#)> (accessed on 29th August 2026).

¹² Sec 79(1)–(3), Information Technology Act 2000, available at <[India Code – Information Technology Act, 2000](#)> (accessed on 29th August 2026).

¹³ Ministry of Electronics and Information Technology (MeitY), 'Advisory to Social Media Intermediaries to Identify Misinformation and Deepfakes' (7 November 2023), available at <[Press Information Bureau – Government of India](#)> (accessed on 29th August 2026).

¹⁴ Ministry of Electronics and Information Technology (MeitY), *Explanatory Note: Proposed Amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 in relation to Synthetically Generated Information* (22 October 2025), available at <[official MeitY text](#)> (accessed on 30th August 2026).

¹⁵Internet Freedom Foundation (IFF), 'Withdraw the Draft Synthetic Information IT Rules, 2025' (submission to the Ministry of Electronics and

Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules 2026 dated 10 February 2026 which will enter into force on 20 Feb 2026.¹⁶

The 2026 Amendment Rules do four principal things. **First**, they define SGI broadly to cover any content “created, modified or altered by a computer resource in a manner that appears authentic or true”. **Second**, any intermediary enabling the creation or modification of SGI must ensure such content carries a prominent label and permanent, non-removable embedded metadata or an equivalent provenance mechanism, and that this label cannot be stripped by downstream users. **Third**, SSMLs, platforms with over five million registered Indian users, face additional obligations: they must obtain a user declaration on whether uploaded content is synthetic *before* publication, and reject non-compliant uploads. **Fourth**, takedown timelines for unlawful content have been compressed dramatically, to as little as three hours for certain notified categories, with a resident Grievance Officer required to acknowledge complaints within 24 hours and only officers of Joint Secretary/DIG rank or above authorised to issue takedown directions, subject to monthly review at Secretary level.¹⁷

The compliance architecture is built entirely around intermediary due diligence tied to safe harbour, there is still no free-standing statutory right that a deep-faked individual can assert directly against a creator, and no dedicated criminal offence of creating a non-consensual deepfake. Removal or disabling of SGI in compliance with the grievance mechanism is expressly deemed not to violate the intermediary’s safe harbour, which incentivises platforms toward over-removal at the margin, precisely the concern the Internet Freedom Foundation raised.¹⁸

Data Protection and Criminal Liability under the DPDP Act and BNS

The DPDP Act makes consent the default basis under which it is lawful to process personal data, and it is not a stretch to conceive of an individual's face or voice - the grist of any deepfake - as falling within the Act's wide definition of what qualifies for the purpose of processing. In theory at least, a non-consensual gathering or use of an individual's biometric likeness for the purposes of training or operating a deepfake model, could also potentially fall within the remit of the Act, with the same being enforceable by the Data Protection Board of India – though the Board’s operative regulations and readiness are works in progress, and we are yet to see or hear of targeted enforcement actions for any deepfake generators, etc.¹⁹

On the criminal side, the new penal code, namely the Bharatiya Nyaya Sanhita 2023 (“BNS”); will be taking over from Indian Penal Code from July 1st, 2024; retains several offenses of cheating by forgery, defamation, stalking and voyeurism which are broadly similar in spirit to sections under the IPC which have traditionally been invoked in FIRs of deepfakes (sections 465 and 469 IPC have counterparts in BNS sections 336 and 338 and were cited in the FIR concerning the Mandanna actress). Neither sets of offenses, in the IPC or the BNS, was specifically conceived with AI created media in mind, and they would also require courts to read such novel harm into existing provisions.²⁰

Copyright and Personality Rights

Intellectual property may also extend for protection in other laws to the extent that it forms part of one's persona. Performer's right and Moral Rights fall within the ambit of Section 38 and 57 respectively under the Copyright Act, 1957.²¹ However the applicability of the Trademark Act, 1999²² may arise where any persons' name, Mark or any other peculiar characteristic identity used for a certain goods/services is leveraged for commercial purposes.

Information Technology, 13 November 2025), available at <[Internet Freedom Foundation](#)> (accessed on 30th August 2026).

¹⁶Ministry of Electronics and Information Technology, *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026*, G.S.R. 120(E), 10 February 2026, available at <[official MeitY Gazette notification](#)> (accessed on 30th August 2026).

¹⁷ Ministry of Electronics and Information Technology, *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026*, G.S.R. 120(E), 10 February 2026, available at <[Ministry of Electronics and Information Technology \(official Gazette notification\)](#)> (accessed on 30th August 2026).

¹⁸ Internet Freedom Foundation, ‘Withdraw the Draft Synthetic Information IT Rules, 2025’ (15 November 2025), available at <[Internet Freedom Foundation – official submission and analysis](#)> (accessed on 30th August 2026).

¹⁹ Sec 2(t), 4, 6, 7, 18, 27 and 33, Digital Personal Data Protection Act, 2023, available at [India Code – Digital Personal Data Protection Act, 2023](#) (accessed on 30th August 2026).

²⁰ Sec 336, 356, 77 and 78, Bharatiya Nyaya Sanhita, 2023, available at <https://www.mha.gov.in/sites/default/files/250883_english_01042024.pdf> (accessed on 30th August 2026).

²¹ Sec 38 and 57, Copyright Act 1957, available at [Copyright Office, Government of India – Copyright Act, 1957](#) (accessed on 30th August 2026).

²² Sec 29 and 30, Trade Marks Act 1999, available at <[India Code – Trade Marks Act, 1999](#)> (accessed on 30th August 2026).

Hence, a right to Privacy the locus classicus from *K.S. Puttaswamy v Union of India*²³ wherein the Hon'ble Supreme Court has articulated a multifaceted understanding that includes personal liberty, dignity, bodily autonomy as also control over one's information so much so that one could include it in intellectual property as well by way of right to Privacy that would serve to this need besides general concept of Passing Off & unfair competition law.

Building on this legal foundation, Indian courts, particularly the Delhi and Bombay High Courts, have increasingly recognised the need to protect individuals from the unauthorised commercial or digital use of their identity. In such cases, courts have also relied on John Doe or "Ashok Kumar" orders, which allow them to restrain not only the persons already identified as infringers but also unknown individuals who may later violate the claimant's rights. Such orders have been passed in cases involving several public figures, including Amitabh Bachchan, Anil Kapoor, Arijit Singh, Jackie Shroff, Asha Bhosle, Akshay Kumar, Shilpa Shetty and Aishwarya Rai Bachchan. The scope of this protection has also expanded beyond traditional film and entertainment personalities, as reflected in the proceedings involving entrepreneur Aman Gupta.

These developments are particularly relevant to the growing problem of deepfakes. Unlike conventional forms of infringement, deepfakes can reproduce or manipulate a person's face, voice, name or overall likeness and distribute the resulting content rapidly across digital platforms. The existing judicial approach to personality rights therefore provides an important legal basis for individuals seeking to prevent or remove such unauthorised use of their identity.

The Election Commission and Deepfakes during Elections

With India's general and state elections taking place alongside the rapid growth of generative AI tools, concerns over the use of synthetic media in political campaigns have also increased. In this context, the Election Commission of India issued an advisory on the responsible use of Synthetic and Generative AI (SGI) during elections, shortly after the Draft Amendment Rules were published in October 2025. The advisory called upon political parties and candidates to clearly label AI-generated campaign material and avoid using synthetic media in a manner that could misrepresent or mislead voters about political opponents.²⁴

However, the advisory does not have an independent statutory basis. Its authority primarily derives from the Election Commission's constitutional powers under Article 324 and the provisions of the Representation of the People Act, 1951. As a result, its practical impact has largely depended on voluntary compliance by recognised national and state political parties.²⁵

Case Studies

The three case studies below are chosen not simply because they are well known, but because each is doctrinally significant for *both* sides of the deepfake debate, for the individuals and rights-holders harmed by synthetic media, and for the platforms, AI developers and (in the third case) the State whose conduct or inaction is under scrutiny.

Anil Kapoor v Simply Life India & Ors (Delhi High Court, 2023), India²⁶

Citation: CS(COMM) 652/2023 and I.A. 18237/2023–18243/2023, order dated 20 September 2023 (Prathiba M. Singh J).

Facts: The actor Anil Kapoor sued nineteen defendants for the unauthorised commercial exploitation of his name, voice, image, signature and catchphrase "jhakaas", including websites and applications using face-morphing and AI tools to generate fake videos and merchandise bearing his likeness. Advocates Pravin Anand and Ameet Naik, appearing for Kapoor, specifically drew the Court's attention to defendants using generative AI and "dark patterns" to imply a false endorsement.

Holding: The Court granted an ex parte, omnibus injunction restraining the named defendants and "the world at large" from using Kapoor's persona through any means, including artificial intelligence, face-morphing and GIFs, for commercial or personal gain, and directed the Department of Telecommunications and MeitY to block infringing websites. Justice Prathiba M. Singh observed that "the technological tools that are now freely available

²³ Justice K.S. Puttaswamy (Retd.) v Union of India (2017) 10 SCC 1, available at < [Supreme Court of India- Official Judgment](#) > (accessed on 30th August 2026).

²⁴ Election Commission of India, 'Advisory to Political Parties on Responsible and Ethical Use of Artificial Intelligence (AI) during Elections', available at <[Election Commission of India - Official Notification](#)> (accessed on 30th August 2026)

²⁵ Representation of the People Act 1951, available at <[India Code – Representation of the People Act, 1951](#)> (accessed on 30th August 2026).

²⁶ Anil Kapoor v Simply Life India & Ors, CS(COMM) 652/2023, Delhi High Court, order dated 20 September 2023, available at <https://delhihighcourt.nic.in/app/showlogo/100025571715184881134_27822_6522023.pdf/2024> (accessed on 30th August 2026).

make it possible for any illegal and unauthorised user to use, produce or imitate any celebrity's persona, by using any tools including Artificial Intelligence," and that the celebrity's right of privacy is engaged where AI is used to portray his image or voice in a "dark or grim manner".

The Rashmika Mandanna Deepfake and the Regulatory Response, India

Citation: FIR registered under IPC 1860, Section 465 and 469, IT Act 2000, Section 66C and 66E at PS Special Cell (IFSO Unit), Delhi Police dated 10-11-23.²⁷

Facts: A video of a British-Indian social media influencer was manipulated through digital technology to include the face of actor Rashmika Mandanna and the deepfake showing her seemingly walking into a lift while wearing an allegedly immodest garment subsequently went viral on X and other platforms in days. Suo motu proceedings by the Delhi Commission for Women led them to write to Delhi Police who filed an FIR against an unknown online, requested Meta for details about the relevant account, and later arrested the downloader who had purportedly intended to expand an unofficial fan page with it (although he was not the original author of the face-swapping AI technology).²⁸

Outcome and significance: Rather than a civil persona rights action, this criminal proceeding leveraged forgery and identity-theft sections for a use they were never designed for.

It is for this regulatory rather than judicial reason that it is so significant, as the vocal condemnation from the public was swift to prompt the first of MeitY advisories to intermediaries about deepfakes within weeks, kick-starting the regulatory response chain from advisories, drafts of rules to the 2026 Amendment Rules two years later.

Chaitanya Rohilla v Union of India (Delhi High Court, 2023–ongoing), India

Citation: W.P.(C) 15596/2023, heard together with a connected writ petition filed by journalist Rajat Sharma (Manmohan ACJ and Tushar Rao Gedela / Manmeet PS Arora JJ).²⁹

Facts: Advocate Chaitanya Rohilla has recently instituted a public interest litigation in December, 2023 requesting an order directing the union government to identify and disable access to websites/software allowing the creation of deepfakes, seek "dynamic injunctions" for content which infringes upon rights, and implement detailed guidelines for regulating Artificial Intelligence. The similar demands are present in the related petition by India TV, the editor-in-chief of which requested that the intermediaries take-down period of 72 (at the then time) be reduced further.

Judicial observations and outcome: The Division Bench repeatedly expressed alarm at the pace of the technology, remarking at one hearing, "I am shocked that what I can see with my own eyes, and hear with my ears, is fake," and at another that deepfake technology "is going to be a serious menace in the society" and that "the antidote for Artificial Intelligence would be technology only."³⁰ Rather than adjudicate the petitioners' specific demands itself, the Court repeatedly directed the Union Government, through MeitY, to constitute expert sub-committees, take stakeholder input from social media intermediaries such as Meta and X, and file periodic status reports, extending the timeline for a final committee report on more than one occasion; the matter remained pending as the 2025 Draft and 2026 Amendment Rules were being finalised.

Grok / xAI Litigation (United States, United Kingdom and France, 2025–ongoing), Foreign

Background: In December 2025, xAI enabled an in-app image-generation and editing feature on X, allowing any premium user to tag @grok and request an image be created or edited. Within weeks, researchers and journalists documented mass production of non-consensual sexualised deepfakes; more than 1.8 million sexualised images of women were generated in a single nine-day period between 31 December 2025 and 8 January 2026 alone, and over

²⁷Delhi Police IFSO Unit, FIR dated 10 November 2023; reported in Business Today, 'Rashmika Mandanna Deepfake Case: Four Suspects Tracked by Delhi Police' (20 December 2023), available at

<<https://www.businesstoday.in/latest/trends/story/rashmika-mandanna-deepfake-case-four-suspects-tracked-by-delhi-police-search-on-to-nab-key-conspirator-410146-2023-12-20>> (accessed on 30th August 2026).

²⁸The Print, 'Delhi Police Act in Rashmika Mandanna Deepfake Video Case, File FIR' <<https://theprint.in/india/delhi-police-act-in-rashmika-mandanna-deepfake-video-case-file-fir-obtain-details-from-meta/1841559/>> (accessed on 30th August 2026).

²⁹Chaitanya Rohilla v Union of India, WP(C) 15596/2023, Delhi High Court <<https://repository.nls.ac.in/cgi/viewcontent.cgi?article=2377&context=nlsir>> (accessed on 30th August 2026).

³⁰Deccan Herald, 'Deepfake Technology Going to be Serious Menace, Says Delhi HC' (2024). <<https://www.deccanherald.com/india/deepfake-technology-going-to-be-serious-menace-says-delhi-hc-3167446>> (accessed on 30th August 2026).

4.4 million images in total by mid-January, of which as much as 41% contained sexual imagery.³¹ On 8 January 2026, rather than disabling the feature, xAI began limiting free image generation to paying subscribers, a decision plaintiffs characterise as monetising, rather than curbing, the abuse.

Litigation: By August 2026, xAI faced at least six significant proceedings. Ashley St Clair, an individual plaintiff, sued xAI in New York in January 2026, alleging Grok generated sexually explicit images of her including some based on a photograph taken when she was a minor, and pleading intentional infliction of emotional distress and product-design defect. A proposed class action was filed in South Carolina the same month by a woman whose non-consensual image had to be reported repeatedly before removal, and a federal class action was filed in California in March 2026 (amended July 2026) on behalf of minors whose family and school photographs were converted into sexualised material, in one instance producing roughly seven thousand images from a single source photograph.³² In the United Kingdom, Labour MP Jess Asato filed a High Court claim in June 2026 alleging Grok produced deepfakes depicting her in a sexual assault. This culminated in January 2026, when California's Attorney General sent X a cease and desist letter. Later that month, a group of thirty-five attorneys general sent X a letter complaining about its security measures, and that February, French prosecutors launched criminal proceedings against the company and raided X's Paris office. Independent investigations by August 2026 estimated the confirmed number of victims to be 15,736 people in 821 confirmed events, with the majority of traced synthetic-media abuse files occurring from the use of Grok in the first half of 2026.

A Note on Getty Images v Stability AI [2025] EWHC 2863 (Ch)

Although the focus of this Part is the three case studies above, brief mention should also be made of the UK High Court's decision in *Getty Images (US) Inc & Ors v Stability AI Ltd*, handed down on 4 November 2025, since it is the clearest illustration internationally of how classical copyright doctrine strains against the AI-training-data problem.³³ Getty abandoned its primary copyright infringement claims mid-trial; on the surviving secondary infringement claim, the Court held that Stable Diffusion's model weights do not constitute "infringing copies" because no reproduction of the training images is "stored" in the trained model, while finding narrow, historic trade mark infringement where certain early model outputs reproduced Getty's visible watermark, causing a likelihood of confusion as to authorised licensing.³⁴ The result is widely read as a partial win for AI developers and a signal that rights-holders will need either legislative reform or a different doctrinal route, such as unfair competition, database rights, or a text-and-data-mining licensing regime, to meaningfully police the use of their creative works in AI training.

Conclusion

Three years separate the Rashmika Mandanna deepfake from the Grok controversy, and in that time, India has moved from a purely reactive advisory regime to a statutory, if still incomplete, framework under the 2026 Amendment Rules, propelled less by proactive policymaking than by sustained judicial pressure in litigation such as *Chaitanya Rohilla v Union of India* and a rapidly expanding line of personality-rights injunctions typified by *Anil Kapoor v Simply Life India*. The comparative picture shows India is not alone in improvising: the EU has chosen deployer-side transparency, the US is litigating its way toward product-liability standards through cases like the Grok lawsuits, the UK is testing the limits of copyright doctrine in *Getty v Stability AI*, and China alone has attempted a comprehensive, consent-first administrative scheme since as early as January 2023. What unites every jurisdiction, including India, existing legal categories, forgery, copyright, trade mark, tort, intermediary safe harbour, were not built for synthetic media, and each is being stretched, sometimes awkwardly, to cover harms it was never designed to address. Whether India's 2026 Rules mark the beginning of a coherent statutory response, or merely the latest stopgap before the next viral controversy forces the next round of reform, the gaps are identified a free-standing personality right, calibrated criminal offences, cross-border enforcement capacity, and a genuine victim-redress mechanism, are addressed before, rather than after, the next crisis.

³¹Robert King Law Firm (n 15); ClassAction.org, 'Grok Lawsuit Alleges xAI Has Intentionally Capitalized on Sexually Explicit, Non-Consensual AI Deepfakes' <<https://www.robertkinglawfirm.com/mass-torts/grok-lawsuit/>> (accessed on 30th August 2026).

³²LawsuitInformer.com, 'Grok and xAI Lawsuits: AI Deepfake Image Claims Explained' <<https://lawsuitinformer.com/grok-lawsuits>> (accessed on 30th August 2026).

³³Getty Images (US) Inc & Ors v Stability AI Ltd [2025] EWHC 2863 (Ch).

³⁴Bird & Bird, 'Stability AI Defeats Getty Images Copyright Claims in First-of-its-Kind Dispute' (November 2025); Ropes & Gray LLP, 'Getty Image Loses Copyright Infringement Claim Against Stability AI' <<https://www.twobirds.com/en/insights/2025/uk/stability-ai-defeats-getty-images-copyright-claims-in-first-of-its-kind-dispute-before-the-high-court>> (accessed on 30th August 2026).