
DEEPPAKES AND PERSONALITY RIGHTS: LEGAL CHALLENGES ON SYNTHETIC MEDIA REGARDING DEFAMATION, PRIVACY AND NON-CONSENSUAL EXPLICIT CONTENT

KM Vinita¹

ABSTRACT

Deepfake technology AI-generated videos, images or audio that convincingly misrepresent real individuals has surged in sophistication and availability. This poses acute challenges to existing legal regimes governing reputation, privacy, personality rights and sexual content. This article examines these challenges across multiple jurisdictions, notably the US, UK, EU, India and others, using a traditional doctrinal methodology to identify and analyse applicable statutes, case law and legal principles. We explore how defamation law treats deepfakes as false statements, how data protection and privacy law apply to synthetic likenesses, how personality/publicity rights may be infringed by AI-generated use of one's image or voice, and how sexual and non-consensual explicit deepfakes fit under "revenge porn" and criminal statutes. We review leading legislation and judgments, for example, the UK's Online Safety Act 2023 and Data Use and Access Act 2025, France's 2024 SREN law and Criminal Code amendments, Australia's 2024 Criminal Code deepfake amendments, India's 2025 IT Rules amendment, and the patchwork of US state laws, and discuss enforcement and technological constraints. Key findings include the inadequacy of traditional defamation and privacy frameworks to capture deepfakes in some jurisdictions, a trend toward new criminal offences specifically targeting non-consensual deepfake pornography, and stark differences in platform liability e.g. US Section 230 immunity vs. the EU's incoming Digital Services Act). We conclude with comparative tables of legal regimes and remedies, a timeline of key legislative actions, and practical recommendations for legislators, courts, platforms and individuals to strengthen protections while balancing free expression.

Keywords: Deepfakes, Personality Rights, Synthetic Media, Privacy, Non-Consensual Explicit Content.

¹ KM Vinita, Research Scholar, Dr. Bhimrao Ambedkar University, Agra.

Introduction

“Deepfakes” a portmanteau of “deep learning” and “fake” are audiovisual works (videos, images or audio) created or manipulated by AI to depict events or statements that never actually occurred. For example, generative adversarial networks (GANs) can swap one person’s face onto another in a video, or synthesise a public figure’s voice to say anything. These technologies blur reality and fiction in ways often indistinguishable to casual observers.² As senior privacy officials note, AI content generation has enabled “the creation of non-consensual intimate imagery, defamatory depictions...featuring real individuals”.³ In practice, deepfakes have been used for pornographic exploits replacing faces in sexual videos, political misinformation, celebrity impersonation, identity fraud and harassment. A cybercrime alert from US agencies warns that accessible AI tools have made mass production of fake media easy on “no more than a personal laptop and a minimal amount of technical skill”. Compounding the challenge is that high-quality deepfakes are *hard to detect*, often virtually indistinguishable from authentic media, meaning victims may not even know when they occur.⁴

These developments raise urgent legal issues about personality rights. Defamation law libel and slander traditionally protects reputations from false factual statements, but does it cover an AI-generated image or video in which a person is misrepresented? Privacy and data protection laws protect individuals against unauthorised use of their likeness or personal data could a deepfake be treated as processing of personal data without consent? Many countries recognize a “right of publicity” or similar personality right – do AI-created impersonations violate it? And the phenomenon of “revenge porn” the non-consensual sharing of intimate images, has already led to new statutes in several jurisdictions; will these be extended to cover deepfake pornography?⁵

This article employs a doctrinal legal methodology, surveying relevant statutes, case law, and scholarly commentary across jurisdictions, and synthesizing the governing legal rules and

² Nika Nour, *Deepfakes: A Digital Transformation Leads to Misinformation* (September 20, 2026) https://www.academia.edu/82422566/Deepfakes_A_Digital_Transformation_Leads_to_Misinformation.

³ *Ibid*

⁴ Vasist, Pramukh & Krishnan, Satish, *Deepfakes: An Integrative Review of the Literature and an Agenda for Future Research*, Communications of the Association for Information Systems, 590-636 (2022)

⁵ By VMLS Editorial, *Personality Rights in India: The Law Behind AI Cases*, Vinayaka Mission's Research Foundations, (September 21, 2026) <https://vmls.edu.in/blogs/personality-rights-india-ai-deepfakes-law>.

reasoning. We compare how common law and civil law systems approach the problems, citing leading examples. In the United States, for instance, state courts would assess a defamation deepfake under that state's libel laws, often requiring proof of falsity and harm, while federal law, Section 230, largely shields online platforms from user content liability. In the UK and EU, a deepfake could implicate the Defamation Act 2013 or GDPR-based privacy rights. In India, existing BNS provisions on defamation and the IT Act's obscenity and privacy sections may apply. We also consider policy and enforcement issues, for example, balancing free speech and innovation against harm, and the technical limits of detection and catalogue the remedies being proposed (injunctions, damages, content takedown, criminal penalties, platform regulation).⁶

Defamation and Deepfakes

Legal framework: Defamation law protects reputation by allowing a plaintiff to sue if false statements of fact harm their good name. In common-law jurisdictions like the US and UK, defamation libel/slander is a tort; in some civil-law countries, it is also a crime. A key question is whether an AI-manipulated image/video can count as a "statement" for defamation. Courts generally require the plaintiff to show that the content asserted or implied a false and defamatory fact. For example, in the US, a visual depiction might be actionable if it implicitly states a false fact, "this person committed crime X," by video. However, mere portrayal, without commentary, is legally tricky. Some US courts hold that deepfaked images *may* be defamatory if an ordinary viewer would interpret them as conveying false factual content. But many defamation suits fail if the medium is deemed artistic or satirical parody.⁷

International examples: In the US, there is yet no landmark "deepfake defamation" case. Existing torts like false-light invasion of privacy have been used, though several states, *e.g.* New York, have abolished false-light claims. One recent federal advisory note state that state defamation laws *could* apply to deepfakes, but plaintiffs must overcome higher hurdles (*e.g.* proving knowledge of falsity, or actual malice for public figures. California's law AB 602 (2022) specifically targets non-consensual pornographic deepfakes as a new crime, but *defamation* claims would still proceed under normal libel statutes. In the UK, the Defamation Act 2013 requires that a claimant prove

⁶ Bluebook 21st Edition.

⁷ Nalin Mashiwal, *Defamation and freedom of speech under tort law*, ipleaders, (September 21, 2026) <https://blog.ipleaders.in/defamation-and-freedom-of-speech-under-tort-law/>

“serious harm” to reputation; a deepfake alone could meet this if widely circulated, but the claimant must link it to reputational damage. The UK courts have traditionally allowed injunctive relief and damages for digital misrepresentations, cf. the privacy case *Terry v. Person Unknown*.⁸ In India, criminal defamation under BNS 356 does not explicitly mention images, but courts may interpret “spoken or written words” broadly. Both Indian civil and criminal defamation require false statements.⁹ In civil suits, courts could recognise deepfakes as evidence of false publication if the plaintiff shows it was made public.

Related principles: Deepfake defamation invokes core speech- and evidence-rules. For instance, courts will distinguish fact from opinion or satire: a clearly tagged AI parody likely isn’t defamatory. Digital evidence rules also come into play: often deepfakes are anonymous, posing problems for identifying the defendant. Additionally, many defamation regimes (notably the US First Amendment) protect parody and require *actual malice* for public figures, which may immunize some deepfakes as protected speech. On the other hand, deepfakes can escape traditional defenses: even “truth” is no defense if the event never occurred, and attribution can be obscured.¹⁰

Policy considerations: Defamation law balances reputation against free speech. Deepfakes intensify this tension: on one hand, fictional media can be creative expression; on the other, a deepfake can smear reputations at scale. The law typically errs on protecting reputation if a deepfake is objectively defamatory and distributed as truth. However, broad new restrictions on AI-generated speech risk chilling political satire. Some commentators suggest tailored rules.¹¹

Privacy and Data Protection

Legal framework: Privacy law encompasses several distinct protections. One strand is information privacy: misuse of personal data. In the EU and UK, the GDPR and Data Protection Acts treat images of identifiable persons as personal data. Processing such data (creating or distributing a deepfake from real images) without consent typically violates data protection rules.

⁸ Frankie Peck, *Deepfake victim urges better regulation of 'dangerous' AI*, (September 21, 2026) <https://www.bbc.com/news/articles/c75gvyk6d4yo>.

⁹ Bhartiya Nagrik Sanhita, 2023, S. 356.

¹⁰ Advocate Siddharth Gupta, *AI-Generated Deepfake Defamation: Legal Remedies Under IT Act & BNS (Calcutta HC Perspective)*, (September 21, 2026) <https://siddharthgupta.in/blog/ai-deepfake-defamation-legal-remedies-calcutta-hc>

¹¹ *Ibid.*

In common law jurisdictions like the US, there is no comprehensive federal privacy law, but many states recognize torts like intrusion or misuse of one's name/likeness. Another strand is privacy of personal life, private facts, image rights and space/privacy no recording in private. Deepfakes are novel here: they do not capture actual private events, but they *fabricate* a person's image/voice.¹²

International examples: EU law is robust. The GDPR's definition of personal data includes any photograph by which someone is identifiable. Thus, generating a deepfake from photos involves "processing" of personal data by "automated means". Absent a legitimate basis e.g., consent, this contravenes Articles 6 and 9 of the GDPR. Moreover, the EU's upcoming AI Act, adopted 2025, specifically imposes transparency obligations on AI-generated content – deepfakes used publicly would need clear labelling to be legal. In the UK, the Data Protection Act 2018 incorporating GDPR similarly covers images. A person could sue the creator of a deepfake for unlawful processing of biometric data if the AI used features like face recognition, which is a special category, or for misuse of data. For instance, if an AI app scraped one's social media pictures to create explicit deepfake porn, regulators and courts could view that as a breach of data protection.

Privacy and Data Protection in Indian Law

Right to Privacy under Article 21

The constitutional foundation should begin with **Article 21 of the Constitution of India**. In *Justice K.S. Puttaswamy (Retd.) v. Union of India*,¹³ the nine-judge Bench of the Supreme Court unanimously recognised privacy as a constitutionally protected fundamental right, arising principally from life and personal liberty under Article 21 and also connected with dignity and other Part III freedoms. The Court treated bodily privacy, informational privacy, decisional autonomy and control over personal information as important dimensions of privacy.¹⁴

This doctrine is especially relevant to deepfakes. An AI-generated intimate image or video may be entirely fabricated, yet it can appropriate a person's face, voice, body, identity and sexual

¹² Adhithi V Bhattathiri et al. all, *Deepfake in the Courtroom: Legal Challenges and Evidentiary Standards*, Digital Doppelgangers: The Rise of Deepfakes & Artificial Intelligence (2025).

¹³ AIR 2017 SUPREME COURT 4161, (2017)

¹⁴ India Const. Art. 21.

persona without consent. The privacy injury therefore does not necessarily depend upon whether the depicted event actually occurred. Synthetic intimate content can interfere with dignity, autonomy and an individual's ability to control the presentation of their identity.

Puttaswamy is particularly useful because the Court also recognised that technological developments generate new privacy concerns and that constitutional interpretation must be capable of responding to technological change. It further held that State interference with privacy must satisfy requirements including **legality, legitimate State aim/need, and proportionality**.¹⁵

Copyright and AI-Generated Deepfakes

The **Copyright Act, 1957** becomes relevant from two different perspectives: the copyright status of AI-generated output and the unauthorised use of copyrighted source material to construct synthetic content.¹⁶ Section **2(d)(vi)** is particularly important. For a literary, dramatic, musical or artistic work that is **computer-generated**, the Act identifies the author as “*the person who causes the work to be created*.”¹⁷

However, applying this provision to modern generative AI is not straightforward. Indian copyright legislation predates generative-AI systems, and there is not yet binding Indian precedent conclusively determining how Section 2(d)(vi) applies to contemporary AI-generated works. Questions therefore remain concerning who “causes” the work to be created, the necessary degree of human creative contribution, originality, ownership and whether purely autonomous AI output attracts copyright at all.¹⁸

New Criminal Laws: BNS and BSA

¹⁵ Justice K.S.Puttaswamy(Retd) And Anr. vs Union of India And Ors., (September 25, 2026) <https://indiankanoon.org/doc/127517806/>

¹⁶ The Copyright Act, 1957

¹⁷ *Id.* S. 2(d)(vi).

¹⁸ *Ibid.*

The **Bharatiya Nyaya Sanhita, 2023 (BNS)** does not create a standalone offence called “deepfake.” Nevertheless, several provisions can become relevant depending upon how synthetic content is created, used and distributed.¹⁹

Section **77 BNS (Voyeurism)** criminalises specified conduct involving watching or capturing the image of a woman engaging in a private act and dissemination of such an image. Significantly, where capture is consensual but dissemination to third persons is not, dissemination can still constitute an offence under the provision. Section **78** addresses stalking, including monitoring a woman's use of the Internet, email or other electronic communication. Section **79** also addresses specified conduct intended to insult the modesty of a woman, including intrusion upon her privacy.²⁰

Depending on the facts, other BNS offences including those concerning defamation, cheating, personation, intimidation, forgery or sexually explicit conduct may require examination in a deepfake case. The important doctrinal point is that liability must be mapped to the elements of the particular offence rather than assuming that every malicious deepfake automatically falls within one BNS provision.

The **Bharatiya Sakshya Adhiniyam, 2023 (BSA)** raises a different but equally important problem: Can a court trust digital material when AI can fabricate convincing audio, images and video?²¹

Section **61** expressly provides that an electronic or digital record cannot be denied admissibility merely because it is electronic or digital, subject to Section 63, and gives such records the same legal effect, validity and enforceability as other documents.²² Sections **62–63** govern proof/admissibility of electronic records.²³

This provides an excellent analytical point for your paper: AI does not merely create new offences or harms; it creates an evidentiary authenticity problem. Courts increasingly need to

¹⁹ The Bharatiya Nyaya Sanhita, 2023

²⁰ *Id.* S.77.

²¹ The Bharatiya Sakshya Adhiniyam, 2023.

²² *Id.* S.61.

²³ *Id.* S.61-63.

distinguish genuine electronic evidence from manipulated or AI-generated material. Questions of provenance, metadata, chain of custody, forensic examination and authenticity consequently become central.

Information Technology Act, 2000 and Deepfakes

The **Information Technology Act, 2000**, as amended, should be discussed alongside the BNS rather than replaced by it. Particularly relevant provisions include **Section 66E** concerning violation of privacy,²⁴ **Sections 67 and 67A** concerning electronic publication/transmission of obscene and sexually explicit material, and the intermediary liability framework under **Section 79**.²⁵

For non-consensual sexual deepfakes, this combination is particularly significant. Depending upon the factual circumstances, the same act may engage constitutional privacy and dignity, criminal-law provisions, IT-law provisions, copyright interests and civil/personality-right remedies.²⁶

Indian case-law structure

K.S. Puttaswamy should be the constitutional anchor. The judgment expressly connects privacy with dignity, autonomy, bodily integrity and control over personal choices, while recognising that technological developments require privacy doctrine to remain adaptable.²⁷

Indian law does not yet regulate deepfakes through a single comprehensive deepfake statute. Instead, legal protection is dispersed across constitutional privacy, criminal law, information-technology law, evidence law, copyright and personality-right jurisprudence. The principal difficulty is not a complete absence of legal remedies, but fragmentation and the

²⁴ The Information Technology Act, 2000, S. 66E.

²⁵ *Id.* S.79.

²⁶ *Ibid.*

²⁷ *Supra* Note 12.

challenge of applying laws developed for conventional conduct to synthetic media capable of manufacturing apparently authentic representations of a person's face, voice and identity.²⁸

*R. Rajagopal v. State of Tamil Nadu (Auto Shankar case)*²⁹, This is one of the foundational Indian privacy decisions. The Supreme Court recognised the citizen's right to safeguard the privacy of personal life and described privacy in terms of a “right to be let alone.” It is an important bridge between Article 21 privacy and later personality-right jurisprudence. The decision has subsequently been relied upon in personality-right cases.³⁰

Justice K.S. Puttaswamy (Retd.) v. Union of India,³¹ The nine-judge Bench constitutionally affirmed privacy as a fundamental right. For deepfake research, the judgment is crucial because privacy is connected with **dignity, autonomy, identity and informational self-determination**. It provides the constitutional foundation for arguing that unauthorised synthetic reproduction of someone's identity can implicate Article 21.³²

D.M. Entertainment Pvt. Ltd. v. Baby Gift House:³³ The Delhi High Court dealt with unauthorised commercial exploitation of singer Daler Mehndi's persona through dolls and recognised protection against commercial appropriation of celebrity identity. It is frequently cited in modern personality-right cases. *ICC Development (International) Ltd. v. Arvee Enterprises*,³⁴ Particularly useful for explaining the conceptual relationship between **privacy and publicity rights**. The Delhi High Court treated the right of publicity as flowing from privacy and as a right associated with an individual rather than an event or corporation. *Titan Industries Ltd. v. Ramkumar Jewellers*,³⁵ An important authority concerning unauthorised commercial exploitation of celebrity identity. It strengthens your discussion of an individual's control over the commercial use of personality attributes.

²⁸ *Ibid.*

²⁹ (1994) 6 SCC 632

³⁰ *R. Rajagopal v. State of Tamil Nadu*, 1994) 6 SCC 632

³¹ *Supra* Note 12.

³² *Ibid.*

³³ 2010 SCC OnLine Del 4790

³⁴ 2003 (26) PTC 245 (Del)

³⁵ (50) PTC 486 (Del) 2012

Amitabh Bachchan v. Rajat Nagi:³⁶ The Delhi High Court protected Amitabh Bachchan's personality attributes from unauthorised exploitation. This case is important as a direct predecessor to the more explicit AI/deepfake cases that followed; the Bombay High Court later cited it in *Arijit Singh. Anil Kapoor v. Simply Life India & Ors.*,³⁷ This should be one of your **principal cases**. The Delhi High Court addressed misuse of Anil Kapoor's name, image, likeness, voice and other identifiable personality attributes. The decision has become an important authority for applying personality/publicity rights to technologically enabled misuse. ***Mrs X v. Union of India***, Delhi High Court,³⁸ Extremely useful for your section on **non-consensual intimate content**. The Delhi High Court issued directions concerning dissemination and repeated circulation of non-consensual intimate images online and addressed responsibilities of authorities and intermediaries. Although not simply a “deepfake case,” it provides an important doctrinal bridge between privacy, sexual autonomy, victim protection, intermediary responsibility and synthetic intimate imagery.

Jaikishan Kakubhai Saraf alias Jackie Shroff v. The Peppy Store & Ors.,³⁹ The proceedings concerned unauthorised exploitation of Jackie Shroff's name, image, voice and other personality attributes, including technologically enabled uses. In 2026, the Delhi High Court granted a permanent injunction protecting his personality rights across physical and digital media, including AI-generated uses.

Arijit Singh v. Codible Ventures LLP & Ors.,⁴⁰ This is especially important for your **AI-generated voice and copyright/personality-right discussion**. The Bombay High Court restrained unauthorised exploitation of Arijit Singh's name, voice, vocal style, image, likeness and other personality attributes. The protection expressly extended to AI voice models, voice-conversion tools, synthetic voices, digital avatars, generative AI, deepfakes and face morphing. ***Ankur Warikoo & Anr. v. John Doe & Ors.***,⁴¹ Highly relevant because it directly involves deepfakes, AI, personality rights and publicity rights. WIPO's case summary records that Warikoo approached the Delhi High Court concerning unauthorised exploitation of his personality and

³⁶ (2022) 6 HCC (Del) 641

³⁷ 2023 SCC OnLine Del 6914

³⁸ 2023.

³⁹ 2024 SCC OnLine Del 3664

⁴⁰ 2024 SCC OnLine Bom 2445

⁴¹ 2025 SCC OnLine Del 3727

related AI/deepfake uses. **Aishwarya Rai Bachchan personality-rights case**,⁴² Delhi High Court, Particularly valuable for connecting **personality rights directly with privacy and dignity**. The Delhi High Court observed that unauthorised exploitation of personality attributes can involve both commercial exploitation and violation of privacy, thereby undermining the right to live with dignity. The injunction covered AI, generative AI, machine learning, deepfakes and face morphing. **Ravi Shankar v. John Doe(s)/Ashok Kumar(s) & Ors.**⁴³ Delhi High Court, The Delhi High Court protected Sri Sri Ravi Shankar's name, voice, image, likeness and distinctive attributes against unauthorised exploitation. Importantly for your topic, the order expressly extended to AI-generated content, deepfake videos, voice-cloned audio and other technological formats. **Aman Gupta v. John Doe/Ashok Kumar & Ors.**,⁴⁴ This is especially valuable for the non-consensual sexually explicit deepfake dimension of your research. The Court restrained unauthorised exploitation of Gupta's name, likeness, image, voice, photographs, videos and persona through AI/deepfake technologies. The proceedings also involved sexually explicit manipulated content, making the case useful for analysing the intersection between personality rights, privacy, sexual deepfakes and unlawful commercial exploitation.

Personality/Publicity Rights

Legal framework: Many jurisdictions recognise a right of publicity or personality – a person's exclusive right to control commercial use of their name, image or persona. This stems from privacy and property interests: in the US, nearly every state has a statute or common-law rule allowing celebrities and increasingly private individuals to sue for unauthorised commercial exploitation of their likeness. In Europe, civil law countries, *e.g.* France, Germany, often have explicit personality or image rights rooted in human dignity; common-law countries rely on privacy or passing-off law. India has no general publicity statute, but the Image (or name) can be protected via trademark/passing off in limited cases, especially for celebrities or as a species of right to privacy.⁴⁵

⁴² 2025

⁴³ *Ibid.*

⁴⁴ CS(COMM) 462/2026

⁴⁵ Ajay Bhargava and Phalguni Nigam, *The Judicially Crafted Shield: India's Evolving Law of Personality Rights*, SSC Online, (September 22, 2026) <https://www.sconline.com/blog/post/2025/12/05/india-personality-rights-evolving-law-celebrity-protection/>

Deepfake implications: A deepfake uses a person's likeness in arguably non-commercial ways, often malicious or personal, which complicates traditional publicity law, which typically requires commercial endorsement usage. For example, US right-of-publicity laws were designed to stop companies selling products with a celeb's face without permission. If someone creates a false video of a celebrity or private person speaking/spreading rumours, this is not direct "commercial use." Thus, some US courts might not deem it a publicity violation, unless the fake is used to solicit business like, deepfake endorsements. However, a creative theory is that a deepfake about a person is an "unauthorised book" on their persona and could be addressed by publicity or privacy law.⁴⁶

International examples: In California, the right of publicity is broad California Civ. Code § 3344)⁴⁷ and even criminal impersonation laws Cal. Penal Code §528.5 have been cited for deepfakes.⁴⁸ Tennessee's 2024 "ELVIS Act" explicitly added voice-cloning to its publicity rights. In Europe, French civil code protects individual likeness under Article 9 private life; a non-consensual deepfake could fall under this. The French SREN law 2024 also criminalised certain deepfake uses.⁴⁹ In the UK, there is no stand-alone right of publicity image control comes via privacy or copyright. Courts have enforced celebrities' rights over unauthorised use of their image, e.g. injunctions against fake Vogue covers. A deepfake portrait might be challenged under passing-off, misleading association with a brand or breach of confidence if personal images were used.⁵⁰

Case law: Reported cases are scant. One US lawsuit filed in early 2026 alleges deepfake impersonation of reality TV personalities on social media to defraud followers the plaintiffs relied on trademark and publicity statutes. No court has yet decided whether generating a digital likeness can itself be theft of publicity rights. In civil law countries, French courts have long held that image use without consent infringes rights of "personnalité". The recent *Filiation Principautaire* cases hint that unconsented digital reproductions of protected portraits are unlawful. India had a landmark personality-rights judgment in *Bennett Coleman v. K.M. Dayal*⁵¹ recognizing celebrity

⁴⁶ *Ibid.*

⁴⁷ California Civ. Code § 3344),

https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV§ionNum=3344.

⁴⁸ Cal. Penal Code §528.5

⁴⁹ The French SREN law 2024

⁵⁰ AI Deepfakes and Image Rights: How to Protect Your Brand's Likeness in the UK, (September 22, 2026) <https://jamiesonlaw.legal/blog/ai-deepfakes-and-image-rights-how-to-protect-your-brands-likeness-in-the-uk/>

⁵¹ 1973 AIR 106, 1973 SCR (2) 757.

image rights, which could analogously cover deepfakes if viewed as infringing a personality right.⁵²

Policy and First Amendment: Especially in the US, publicity rights collide with free speech. The First Amendment allows artistic depictions of real people. Courts often carve out broad “newsworthiness” and parody exceptions to publicity claims. Deepfakes raise the question: is a video “parody” or “comment” thus protected speech, or purely commercial exploitation? Current law struggles to answer this for AI media. Critics warn against a “robotic Sherman’s law” against any celebrity likeness in AI-generated content, as this could stifle creativity. However, advocates argue that egregious non-consensual deepfake uses should be curtailed in the name of individual dignity.⁵³

Non-Consensual Explicit Content

The most egregious use of deepfakes has been “revenge porn” or non-consensual pornography. In this scenario, AI is used to superimpose a target’s face onto explicit images or videos without their consent, causing severe humiliation and psychological harm. Many jurisdictions have responded by criminalizing the creation or distribution of intimate images without consent NCII laws. Where deepfakes blur the line, questions arise whether those statutes cover algorithmically generated images.

Legal developments: The last five years have seen a global push to extend NCII laws to cover AI-generated imagery. In the US, nearly all states now have some form of law against non-consensual intimate images. For example, California’s AB 602, effective 2022 explicitly criminalises creating or sharing a sexually explicit image of someone without their consent, “including images which have been digitally manipulated”.⁵⁴ Virginia, Texas, Florida and many others similarly proscribe deepfake porn as a new category of sexual harassment or exploitation. By September 2026, about 48 states had enacted laws addressing deepfake pornography. At the

⁵² *Bennett Coleman v. K.M. Dayal*, 1973 AIR 106, 1973 SCR (2) 757.

⁵³ *Ibid.*

⁵⁴ California’s AB 602 California’s AB 602

federal level, the proposed “TAKE IT DOWN Act” (2026) would make non-consensual deepfake images a crime nationwide with takedown duties on platforms.⁵⁵

In the UK, the Online Safety Act, 2023 modernized revenge porn offences to explicitly include digital alteration. Home Office ministers confirmed that sharing or threatening to share intimate images without consent “including images which have been digitally altered” is now a criminal offence.⁵⁶ Moreover, the **Data Use and Access Act, 2025**, coming into force in early 2026, criminalizes the *creation* or even *request* of non-consensual sexual deepfakes.⁵⁷ This is groundbreaking: a person who simply *uses an AI tool to generate* a pornographic deepfake could face up to 2 years in prison, the same as sharing one.⁵⁸

International examples: Australia passed the *Criminal Code Amendment (Deepfake Sexual Material) Act 2024*. This federal law makes it an offence punishable by up to 6 years’ imprisonment to distribute any sexually explicit material of an identifiable person without consent, expressly covering AI-generated content.⁵⁹ In South Korea, the Sexual Violence Punishment Act was amended in 2024 to penalise producing, sharing or possessing explicit deepfakes, closing loopholes in earlier law.⁶⁰ In the EU, Member States vary: France’s SREN law (2024) forbids non-consensual deepfake pornography unless clearly marked,⁶¹ and imposes harsher penalties for sexual deepfakes (Article 226-8-1 of the Criminal Code. Germany’s recently enacted *NCII Act* (effective 2025) likewise includes digitally-manipulated intimate images in its definition of illegal content.⁶²

Enforcement and remedies: Criminal NCII laws often carry jail terms or fines. Victims can sometimes obtain civil remedies damages, injunctions under general laws. Platforms play a crucial role: under many new regimes like Australia’s eSafety Act and the UK Online Safety Act, social media sites have takedown obligations and can be fined for non-compliance. For instance, Ofcom

⁵⁵ Sharing of Intimate Images Without Consent: Know Your Rights, Office on Violence Against Women (OVW) US Department Justice, (September 22, 2026) <https://www.justice.gov/ovw/sharing-intimate-images-without-consent-know-your-rights>.

⁵⁶ The Online Safety Act, 2023.

⁵⁷ Data Use and Access Act, 2025.

⁵⁸ *Ibid.*

⁵⁹ The Criminal Code Amendment (Deepfake Sexual Material) Act, 2024.

⁶⁰ The Sexual Violence Punishment Act was amended (2024).

⁶¹ France’s SREN law (2024).

⁶² NCII Act (effective 2025).

now has power to investigate and penalise platforms that allow deepfake porn the UK Government explicitly warned tech companies to act quickly to remove *Grok* platform deepfakes, under threat of fines up to 10% of global revenue.⁶³

Related torts/crimes: Deepfake harassment can also fall under existing laws: stalking, hate speech, or harassment statutes might apply if the fake is used to threaten or abuse. In the US, some victims have invoked state cyberharassment laws. Identity theft statutes (where available) may criminalize impersonation for fraud. In India, dissemination of obscene material (IT Act §67) can cover deepfake porn, and new proposals (e.g. “nudification app” bans) are in the works.

Therefore, Non-consensual sexual deepfakes are one area where many jurisdictions have acted swiftly. Explicit crimes now exist in countries like Australia and France, and are being introduced in the US and UK. Civil damages may also be claimed under privacy or abuse of image theories. Nonetheless, enforcement remains challenging: many deepfakes are posted anonymously or abroad. This has prompted powerful regulatory measures (e.g. mandatory age/identity verification for deepfake apps in *Australia*, mandatory content notices in *India*. As one EU privacy statement notes, intimate deepfakes are not just image alterations but tools of abuse, requiring *criminal sanction* and platform accountability.⁶⁴

Technological and Enforcement Challenges

Deepfakes sit at the intersection of law and advanced technology. From a technical view, deepfake creation relies on complex AI like generative adversarial networks) trained on large datasets of images. Detection tools often leverage neural nets or forensic analysis examining eye-blinking, shadows, encoding artefacts, or video consistency. However, detection is a cat-and-mouse game. An NSA/FBI advisory notes that generative algorithms are now *open source and pervasive*, so malicious actors can create highly convincing fakes on a laptop. Meanwhile, defenders warn that deepfakes are becoming “increasingly difficult to detect”, especially as AI

⁶³ Majid Yar and Jacqueline Drew, *Image-Based Abuse, Non-Consensual Pornography, Revenge Porn: A Study of Criminalization and Crime Prevention in Australia and England & Wales*, v. 13 issue 2 International Journal of Cyber Criminology (2019)

⁶⁴ *Ibid.*

improves. Watermarking and provenance standards are proposed, such as the EU's proposed mandatory "synthetic media labelling", but not yet universally adopted.⁶⁵

This technological complexity complicates legal enforcement. Law enforcement may need technical expert testimony to prove an image is fake. Judges and juries might be uncertain about the nature of the evidence. Automated content moderation on platforms is often the first line of defence, but algorithms can generate false positives/negatives. The NSA's Cybersecurity Information Sheet recommends organizations use a combination of real-time verification, passive detection and human review, but acknowledges no perfect solution. Moreover, deepfake creators can often evade detection by adding noise or otherwise fooling detectors.⁶⁶

On the legal side, statutory gaps and ambiguities pose enforcement hurdles. For example, prior to the recent UK laws, it was unclear whether sharing a non-consensual *AI-generated* intimate image was prosecutable. The UK remedied this in 2026 by updating the law mid-session. But in many places, police still lack explicit guidance on these cases. International cooperation is also needed: deepfakes easily cross borders, but criminal enforcement is jurisdiction-bound. The NL Times reports the *first Dutch deepfake prosecution* in September 2026, highlighting new laws there. Even so, the website operator in Canada was not charged because at the time, Canadian law had no such offence, illustrating jurisdictional divergence.⁶⁷

Thus, the technology behind deepfakes challenges both detection and attribution, while the law races to catch up. Courts and regulators must grapple with nuanced evidence and apply laws not written for synthetic media. To date, strategies combine:

- (a) strengthening laws (as seen above);
- (b) relying on general provisions (like copyright, harassment, data protection);
- (c) imposing platform duties (like quick takedown mandates); and

⁶⁵ Alexandros Gazis et. al., *Deepfakes and Synthetic Media: Generation, Detection, and Governance*, Encyclopedia (2026).

⁶⁶ *Ibid.*

⁶⁷ *Ibid.*

(d) encouraging industry solutions (voluntary guidelines, digital watermarking). Each of these has limits. Notably, some tech commentators warn that *total* prevention may be impossible; thus, the legal focus is often on harm control (punishing misuse, compensating victims, and improving awareness) rather than on banning the underlying technology entirely.

Comparative Remedies and Liability

The response to deepfakes varies significantly by legal system. **Table 1** (below) summarises the primary legal provisions and types of relief in key jurisdictions. **Table 2** then outlines the remedies available: injunctions, damages, criminal sanctions, takedown orders and any special platform rules.

Jurisdiction	Defamation Law	Privacy/Data Protection	Publicity/Personality	Non-Consensual Explicit Content	Platform Liability
USA	State libel/slander torts; plaintiff must prove falsity and harm; first amendment defenses strong.	No federal privacy law; various state torts (intrusion, false light) and federal statutes for specific data (health, finance).	Recognized as statutory tort in most states (California Civil Code §3344, etc.), protecting commercial use of likeness.	State laws (now 48 states) criminalize non-consensual pornographic deepfakes; federal law only covers computer-generated child porn (CDAA).	Section 230 Immunity largely protects platforms from user-generated deepfake liability; proposed federal laws (e.g. NO FAKES Act) would

					impose notice-and-takedown duties.
UK	Defamation Act 2013 (serious harm threshold, defenses of truth and opinion). Plaintiffs can seek damages/injunctions.	UK GDPR/Data Protection Act 2018 – images are personal data; processing without consent is unlawful. Also tort of misuse of private information can apply.	No stand-alone publicity statute; personality rights protected via privacy, passing-off, or misuse of confidence.	<i>Online Safety Act 2023</i> : sharing intimate images without consent (even digitally altered) is a criminal offence. <i>Data (Use & Access) Act 2025</i> : creating/seeking non-consensual sexual deepfakes is a new offence.	Online Safety Act imposes duty of care on platforms (especially for the newly defined “priority” harms) and gives Ofcom power to fine/remove non-consensual content. Traditional e-commerce “safe harbor” is limited by

					“actual knowledge” provisions.
EU	No unified rule; national defamation laws (often stricter than US) govern false statements.	GDPR (and e-Privacy) – strong consent and purpose limitations on personal data (includes photos); rights to erasure/correction.	Civil-law personality rights (e.g. France Code civil Art.9) protect image/name. Some states have publicity law (e.g. Germany’s Model IP Law).	Member states have evolving laws: France’s 2024 SREN law explicitly bans non-consensual deepfakes; many countries incorporate digital revenge-porn statutes. The EU AI Act mandates watermarking/transparency for generated media.	Digital Services Act (effective 2024): online platforms must rapidly remove illegal content (including NCII) upon notice. AI Act (2025) imposes transparency obligations (e.g. tagging deepfakes as AI) for

					providers of high-risk systems.
India	IPC §499/500 (criminal defamation); civil suits possible under injunctions/equity. Plaintiff need not be public figure; truth is not an absolute defence.	No dedicated privacy statute yet (PDPA pending); Supreme Court holds privacy as fundamental right. IT Act § 66E/72 restrict voyeurism/breach of confidentiality (but do not explicitly mention deepfakes).	No explicit publicity law. Personality issues handled via trademark/passing-off in limited cases, or through right to privacy.	IT Act §67 punishes publishing obscene content (includes indecent images). Section 67A covers child pornography (including digital). Non-consensual “revenge porn” pending as specific offence, but deepfake porn is generally treated as obscene material.	IT Act §79 provides safe-harbor for intermediaries if rules followed. New IT Rules 2021 (amended 2025) require platforms to label AI-generated content and remove prohibited content swiftly.

Table 1: Comparison of Laws Addressing Deepfake Harms in Key Jurisdictions.

Remedy/Mechanism	USA	UK	EU	India
Injunctions (Civil)	Available in defamation/privacy suits, though pre-publication injunctions are rare (strong free speech concerns).	Commonly granted for defamation and privacy (e.g. gag orders, content removal) to prevent ongoing harm.	Available under national civil procedure (member states may grant orders to remove content).	Available in civil claims (e.g. court orders to remove defamatory/deepfake images).
Damages (Civil)	Yes. Plaintiffs can recover compensatory (and punitive for malice) damages for defamation, privacy invasion, or right-of-publicity claims.	Yes. Victims can claim pecuniary and non-pecuniary damages for libel and misuse of private information.	Yes. Compensation for defamation or privacy breaches; plus GDPR allows fines (paid to state) and data subject compensation.	Yes. Aggrieved persons can seek damages in tort or civil suits (and civil defamation/IPC have fines).
Criminal Penalties	Some state statutes make deepfake pornography a misdemeanor/felony	Criminal offence to share <i>any</i> intimate images without consent under OSA	Varies. France imposes prison/fines for non-	Yes. IPC 499/500 punish defamation. IT Act §§67/67A punish obscenity

	ny. No federal deepfake-specific crime yet (except proposals).	2023; new offence for creating/requesting NCII under DUAA 2025. Revenge-porn laws are in force.	consensual sexual deepfakes. Many countries criminalize child deepfakes. A 2025 EU Directive will require member states to sanction online sexual abuse including deepfakes.	and child porn (covering AI-generated if “obscene”). Cyber harassment is criminalized under IPC 507 (which may cover harassment via images). New laws to address NCII are under consideration.
Content Takedown	No general “deepfake takedown” law. Copyright DMCA takedowns exist for copyrighted media, but not applicable to defam. Some states require disclosure on	Ofcom and courts can order removal of illegal content. Platforms must expeditiously delete NCII when flagged (as per OS Act).	DSA: Platforms must remove illegal content (including NCII and defamation in some states)	IT Act §69 empowers govt agencies to block online content. IT Rules require platforms to remove disallowed AI-generated deepfakes within hours.

	political deepfakes.		within strict timelines.	
Platform Liability	§ 230 CDA grants broad immunity for user content; platforms rarely liable for defam/deepfakes. Ongoing debate; some calls for carve-outs for NCII.	E-Commerce “safe harbor” principle (no liability without knowledge) still applies, but OS Act requires proactive risk mitigation. Offenses apply to platforms hosting deepfakes.	DSA holds large platforms to high duty of care: mandated risk assessment, “notice and action” on illegal content, transparent reporting. Failure incurs heavy fines.	§ 79 IT Act grants conditional safe-harbor (tied to compliance). Platforms must follow IT Rules (grievance officers, swift removal). Safe harbor can be lost for non-compliance.

Table 2: Comparative Remedies and Enforcement Mechanisms.

Conclusion and Suggestions

Deepfakes represent a frontier challenge for personality rights and related law. This review finds that **no single regime yet offers complete protection**. Common threads include:

- i. nations with strong privacy traditions (EU, UK) rely on data and dignity rights to address deepfakes, whereas common-law countries lean on defamation, privacy torts and emerging criminal statutes;

- ii. non-consensual pornographic deepfakes have prompted new explicit offences in many places (Australia, UK, US states, France, etc.);
- iii. platform regulation is increasingly important – e.g. the UK’s Online Safety Act and the EU’s DSA impose duties on social media companies to block illegal synthetic media; and
- iv. enforcement remains difficult due to anonymity and cross-border dissemination of AI content.

Based on the above discussion, we offer the following suggestions:

- **For Lawmakers:** Enact clear statutes that specifically criminalise non-consensual deepfakes, both pornographic and defamatory and provide civil remedies. Ensure laws balance free expression, allowing satire and parody, with proper labelling) against reputational and privacy harms. Consider frameworks like the EU’s AI Act and DSA that impose transparency watermarking and platform accountability for AI-generated content. Harmonise laws internationally where possible, since synthetic media easily crosses borders. In particular, protect *individual autonomy* by criminalising the mere *creation* of malicious deepfakes, as the UK’s 2025 Act does rather than only their distribution.
- **For Courts:** Interpret existing laws flexibly to cover deepfakes. For example, courts should treat AI-generated images as “images” or “data” under privacy statutes. In defamation cases, allow deepfake evidence to count as publications if a reasonable viewer would accept them as factual. Expedite injunctive relief by treating deepfakes as inherently irreparable in reputation. Develop forensic expertise for courts to assess AI-generated evidence.
- **For Platforms:** Adopt strong content moderation for deepfakes. This includes implementing reliable deepfake detection tools, fast-review processes, and user reporting mechanisms for synthetic defamation or porn. Comply proactively with transparency rules: label AI content, be ready for takedown orders, and share data with law enforcement. Platforms should also support “trusted flagger” schemes to help identify illegal deepfakes.
- **For Individuals:** Stay informed. Public figures and private citizens alike should watermark or limit public photos to reduce training data. Be cautious when sharing sensitive images,

since AI needs real data to create fakes. Victims should document and report deepfakes quickly, and seek both legal and technological remedies *e.g.* content removal services).

Therefore, deepfakes require an *all-of-society* approach: updated laws, vigilant enforcement, robust tech solutions, and public education. Governments must keep pace with AI advances – as seen in recent measures worldwide to protect personality rights and public trust. Courts should lean on fundamental principles of consent, truthfulness, and dignity to fill gaps, and platforms must be partners in prevention. Only through coordinated legal reform and pragmatic safeguards can we limit the reputational and personal harms unleashed by this powerful new technology.