DANGERS OF AI TOOLS: NUDITY, PRIVACY AND LIBERTY [A LEGAL AND TECHNICAL ANALYSIS OF INDIA'S REGULATORY RESPONSE AND ITS CONFLICT WITH GLOBAL PRIVACY NORMS]

Mridulendu Ranjan

I. Introduction:

Generative artificial intelligence has collapsed the distance between imagination and image. A photograph lifted from a public Instagram profile can, within seconds and at negligible cost, be transformed into a photorealistic nude, a fabricated video, or a cloned voice indistinguishable from the original. What began as a novelty in visual effects studios is now a mass market capability accessible through a browser tab. The consequence is a new category of harm that sits at the intersection of three distinct legal interests: bodily and sexual dignity, informational privacy, and personal autonomy over one's own likeness.

This article examines that intersection through an Indian legal lens: the statutory and constitutional architecture that has emerged to address AI generated nudity and non consensual synthetic media, the gaps that remain, and the friction that arises when Indian law is measured against global privacy regimes such as the GDPR and the EU AI Act. It draws on real litigation, platform enforcement actions, and legislative developments through mid 2026.

II. The Technology and the Nature of the Harm:

Nudify or undress applications use diffusion based image models, often derived from open source frameworks, to remove clothing from an uploaded photograph while preserving the subject's face. Unlike traditional morphing, the output requires no technical skill and no original explicit material; the harm is manufactured entirely from an innocuous source photo.

The scale is significant. A 2024 lawsuit filed by the San Francisco City Attorney against sixteen such websites disclosed that the named sites had collectively been visited over 200 million times in just the first six months of that year, and described their advertised purpose as generating explicit images of women and girls without consent. Some of these platforms disclosed that free users received a blurred preview, with full images unlocked only on

payment, commercialising the violation itself.

India has not been insulated from this. The November 2023 incident involving actress Rashmika Mandanna, where her face was convincingly grafted onto another woman's body in a viral video, is widely regarded as the trigger for India's current wave of deepfake specific regulation. Since then, reported incidents have diversified: a Bengaluru IT professional was sextortion targeted in mid 2025 using AI generated nude images built from his LinkedIn photograph; election period synthetic audio impersonating political figures, including deceased leaders, has been flagged by the Election Commission; and in early 2026, X's Grok image tool drew regulatory scrutiny in India after being used to generate explicit alterations of real users' photographs, prompting the platform to restrict image editing features for all users pending compliance review.

A useful international comparator is the Meta Oversight Board's July 2024 ruling on two near identical cases, an AI generated nude image of an Indian public figure that Meta initially left up, and a similar image of an American public figure that Meta removed. The Board found the inconsistent treatment problematic and held that both images should have been removed as violations of Meta's harassment and safety policies, irrespective of the artistic framing sometimes used to justify their retention. The episode illustrates a recurring theme: platform enforcement, absent binding law, is inconsistent, reactive, and geographically uneven.

III. The Indian Legal Framework

A. Constitutional Foundation

The starting point is Justice K.S. Puttaswamy v. Union of India (2017), which held that the right to privacy is intrinsic to Article 21 and that informational privacy, including control over one's name, image, and likeness, is a protected facet of that right. Critically, the Court recognised that privacy harms can arise from private, non State actors, not only from government surveillance. This makes Puttaswamy directly relevant to AI generated nudity, where the violator is typically an anonymous individual or a commercial platform rather than the State.

B. Criminal Law: IT Act, POCSO, and the Bharatiya Nyaya Sanhita

Several overlapping provisions apply:

Section 66E, IT Act, 2000 penalises capturing, publishing, or transmitting images of a person's private area without consent, violating privacy.

Sections 67 and 67A, IT Act penalise publishing or transmitting obscene material and sexually explicit material in electronic form.

Section 67B, IT Act specifically targets child sexual abuse material, and was the subject of the Supreme Court's September 2024 ruling in Just Rights for Children Alliance v. S. Harish, which set aside a Madras High Court finding that merely downloading and viewing child pornography fell outside the ambit of POCSO and the IT Act. The Supreme Court held such conduct is very much within reach of these provisions, reinforcing that possession and consumption, not just creation and distribution, attract liability.

Section 294, Bharatiya Nyaya Sanhita, 2023 (replacing Section 292 IPC) addresses obscene material, now the primary criminal law hook for non consensual sexual deepfakes at the Union level, though commentators have pointed out this is a doctrinally awkward fit: obscenity law is oriented toward protecting public morality, not an individual's consent. A deepfake nude is not wrong because it is obscene; many consensual sexual images are equally explicit. It is wrong because the subject never agreed to appear in it. Treating the harm as an offence against decency rather than a violation of personal dignity and autonomy under serves victims and can leave courts asking the wrong question.

POCSO Act, 2012, read with the BNS, governs any synthetic content depicting a minor, regardless of whether the child was ever photographed in a sexual context; the fabrication itself is the offence.

C. The IT Rules and the 2026 Deepfake Amendment

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 have been amended twice in quick succession, first in October to November 2025, and again through a Gazette notification dated 10 February 2026 (effective 20 February 2026), to create India's first dedicated regulatory category: Synthetically Generated Information (SGI), defined as any audio, visual, or audio visual content created or algorithmically altered to appear indistinguishable from a real person or event.

Key operative obligations under the amended Rules include:

1. Mandatory, continuous labelling of AI generated content, with visible or audible disclosure that cannot be removed by the platform or end user, and embedded metadata to trace provenance.

2. Drastically compressed takedown timelines. The general window fell from 36 hours to 3 hours for content flagged by a court order or an officer not below Joint Secretary rank, and to as little as 2 hours for the most sensitive categories, including non consensual deepfake nudity.

3. Upstream prevention duties on platforms offering content generation tools, requiring them to deploy automated technical measures preventing the creation of child sexual abuse material, obscene or privacy invasive synthetic content, and non consensual intimate imagery at the point of generation, not merely at the point of takedown.

4. Loss of safe harbour under Section 79 of the IT Act if a platform fails to label synthetic content or misses the takedown window, directly linking intermediary liability protection to deepfake compliance.

5. Mandatory identity disclosure to law enforcement where a criminal act has been committed using AI tools, addressing the anonymity that has historically shielded deepfake creators.

This marks a structural shift from India's earlier, purely reactive content moderation model toward what regulators describe as preventive architecture, regulating the mechanism of creation, not merely the output.

D. Personality Rights as a Civil Remedy

Alongside criminal and regulatory provisions, Indian courts have developed a parallel civil track through the tort of personality rights. In Anil Kapoor v. Simply Life India (Delhi High Court, 2023) and a comparable order protecting Aishwarya Rai Bachchan, the Delhi High Court restrained unauthorised commercial and AI driven use of a celebrity's name, voice, and likeness, reasoning that the harm lay in the misappropriation of identity and persona rather than in obscenity or falsity per se. This is doctrinally significant because it locates the wrong correctly, in the non consensual use of a person's identity, and offers victims, particularly public figures, an injunction based remedy that is faster than criminal process, though it remains

largely unavailable to private individuals without independent commercial identity value.

E. The Digital Personal Data Protection Act, 2023

The DPDP Act, India's first comprehensive data protection statute, is directly relevant because nudify tools and deepfake generation depend entirely on the unauthorised processing of a data principal's personal data, their photograph. Section 6 requires consent to be free, specific, informed, unconditional, and revocable. AI models that scrape publicly available images and repurpose them into sexualised synthetic content plainly breach the purpose limitation and data minimisation principles that underpin valid consent, even where the original photograph was itself publicly posted.

However, the DPDP Act has real limitations for this specific harm. The version enacted in August 2023 dropped an earlier draft's broad definition of harm, which had explicitly included reputational injury and psychological harm, from the final text. Its enforcement architecture centres on the Data Protection Board of India, oriented toward compliance and penalties against data fiduciaries, not toward the kind of urgent, individual injunctive relief a deepfake victim needs within hours. The DPDP Rules were only notified in November 2025, with full substantive enforcement, including breach notification, consent manager integration, and rights processes, phased in through November 2026 and May 2027. For a victim today, the DPDP Act is a slow moving compliance framework running in parallel to, rather than displacing, the faster criminal and IT Rules remedies.

IV. Conflict with Global Privacy Norms

A. Structural Divergence from the GDPR

India's approach borrows GDPR vocabulary, data fiduciary and controller, data principal and subject, extraterritorial reach, but diverges in ways that matter for cross border AI platforms:

Legal basis for processing. GDPR offers six lawful bases (consent, contract, legal obligation, vital interests, public task, legitimate interests), allowing a three part legitimate interest balancing test to justify processing without consent in defined circumstances. The DPDP Act does not recognise contractual necessity or legitimate interest as standalone bases; consent is the primary ground, narrowed further by a closed list of certain legitimate uses. A global AI company relying on legitimate interest processing for model training under GDPR cannot

transplant that justification into the Indian context without separately securing consent or fitting within India's narrower carve outs.

Sensitive data categories. GDPR creates a heightened protection tier for biometric, health, and similar special category data. The DPDP Act treats all digital personal data, including a face used to train a nudify model, under one undifferentiated standard, which arguably under protects biometric identifiers precisely in the scenario this article addresses.

Children's threshold. DPDP sets the age of a child at 18 uniformly, stricter than GDPR's default of 16 (reducible to 13 by member states). This gives Indian minors broader nominal protection but creates compliance friction for platforms operating a single global consent flow.

Cross border data transfer. GDPR relies on an adequacy decision and Standard Contractual Clause framework. DPDP instead uses a government blacklist model; transfers are permitted by default except to notified restricted countries, which is procedurally more permissive but leaves data fiduciaries with less certainty, since the restricted list can change by executive notification rather than a reasoned adequacy assessment.

Penalty architecture. DPDP penalties are fixed sums up to 250 crore rupees per violation; GDPR penalties scale with global turnover, up to 4 percent. A small Indian nudify app operator and a large multinational platform face the same statutory ceiling in India, which can be disproportionately severe for smaller entities and comparatively lenient for large ones.

B. Conflict with the EU's Labelling Model:

The EU AI Act's Article 50 imposes disclosure obligations on providers of generative AI systems, requiring marking and detection mechanisms for AI generated content and labelling of deepfakes. India's February 2026 amendment goes further procedurally, mandating continuous, non removable, prominent labelling throughout a piece of content's duration, not merely a static disclosure, and couples it with binding takedown timelines the EU framework does not impose in comparable form. A platform operating globally must therefore engineer for India's stricter labelling persistence and shorter takedown clocks as the practical ceiling of compliance, even though its primary regulatory reference point, the EU, is less prescriptive on timing.

C. The US Patchwork and Jurisdictional Reach:

The United States has no federal deepfake statute; the DEEPFAKES Accountability Act remains unenacted, leaving regulation to a growing but uneven set of state laws (California, Texas, Illinois, and others) alongside the San Francisco lawsuit's reliance on state unfair competition and revenge pornography statutes. This fragmentation matters to Indian victims in a very concrete way: many nudify platforms are hosted offshore, often outside India and sometimes outside any jurisdiction with an operative deepfake specific law. India's 2026 takedown timeline obligations bind intermediaries with an Indian nexus, but have limited practical reach over a foreign hosted site with no Indian office, no Indian payment rails, and no incentive to comply, a jurisdictional gap that labelling and takedown rules, however fast, cannot fully close without international cooperation mechanisms that do not yet exist in any binding form.

D. The Underlying Conceptual Conflict:

Beneath these structural differences lies a conceptual one. Global privacy norms, following GDPR, treat the individual's control over their own data as the central value; consent, purpose limitation, and the right to erasure flow from that premise. India's criminal law response to AI nudity, built substantially on obscenity provisions, still partly frames the harm as an offence against public morality. These are not equivalent injuries, and conflating them under a single obscenity label risks a court asking whether content is indecent rather than whether the subject consented, the wrong question for a non consensual deepfake of an otherwise ordinary photograph. India's personality rights jurisprudence and the DPDP Act's consent architecture are, encouragingly, beginning to correct this by anchoring the wrong in autonomy and identity rather than decency, but the correction is incomplete and unevenly applied between well resourced public figures who can obtain quick injunctions and ordinary citizens who cannot.

V. Conclusion and Recommendations:

India's regulatory response to AI generated nudity and privacy harms has moved with unusual speed, three rounds of IT Rules amendments in under eighteen months, a Supreme Court willing to close interpretive gaps in POCSO, and an emerging personality rights doctrine, but it remains a patchwork stitched from criminal law, intermediary rules, and a still maturing data protection statute that will not be fully enforceable before May 2027. For legal practitioners

advising on this space, three points deserve emphasis: first, the criminal remedies (BNS Section 294, IT Act Sections 66E, 67, 67A and 67B, POCSO) provide the fastest recourse for individual victims today; second, the IT Rules' compressed takedown timelines are now the most practically effective tool against platforms with an Indian nexus, but offer little against offshore actors; and third, the DPDP Act, once fully operative, will add a compliance driven deterrent against data fiduciaries but is not designed as an emergency remedy. Harmonising India's framework more explicitly around consent and dignity, rather than obscenity, and building genuine cross border enforcement cooperation remain the two open frontiers.

[*This article is intended for general legal and analytical discussion and does not constitute legal advice on any specific matter*].