Page 4460 - 4482 **DOI:** *https://doij.org/10.10000/IJLMH.1112058*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 2

2026

Deepfake Crimes and AI-Generated Sexual Exploitation in India: Need for Legal Reform

FATMA HAIDER[1] AND SONAKSHI VARSHNEY[2]

ABSTRACT

Rapid advances in AI have given rise to a troubling new dimension of gender-based violence: the non-consensual creation of sexually explicit deepfake imagery. Freely available generative AI tools allow perpetrators to produce realistic fake sexual content featuring real individuals without their consent, with women being disproportionately victimized. This paper examines whether India's existing legal framework, the Information Technology Act, 2000 ; the Bharatiya Nyaya Sanhita, 2023; and the Protection of Children from Sexual Offences Act, 2012 is equipped to address this harm, concluding that it is not. Through doctrinal legal analysis and a comparative study of legislative approaches in the United Kingdom, United States, South Korea, and the European Union, the paper identifies critical gaps: the absence of a consent-centered criminal provision, obscenity laws ill-suited to AI-generated material, inadequate accountability mechanisms for online platforms, and minimal procedural safeguards for those harmed. Drawing on prominent Indian cases and emerging international frameworks, the paper proposes a comprehensive reform agenda that includes a new consent-based criminal offense, accessible civil legal remedies, proactive obligations for digital platforms, and strengthened institutional capacity for enforcement.

Keywords: *Deepfakes, Artificial Intelligence, Non-Consensual Intimate Imagery, Sexual Exploitation, Information Technology Act, Bharatiya Nyaya Sanhita, POCSO, Gender-Based Violence, Platform Accountability, Legal Reform, India.*

I. INTRODUCTION

Among the most urgent legal challenges of the digital era is the growing collision between artificial intelligence and sexual violence. Deepfake technology which refers to audio-visual content fabricated or heavily manipulated through deep learning systems has placed a devastating weapon in the hands of abusers. It allows them to produce startlingly lifelike sexual

[1] Author is a Student at Amity University, Noida, Uttar Pradesh, India.
[2] Author is an Assistant Professor at Amity University, Noida, Uttar Pradesh, India.

 [ISSN 2581-5369]

content featuring real, identifiable individuals, often using nothing more than photographs found freely online. What once would have seemed the stuff of science fiction as recently as 2017 can today be carried out by any person with a smartphone in just a few minutes.

India is acutely vulnerable to this problem. With an internet-using population of over 900 million, and already facing a well-documented crisis of digitally facilitated violence against women, the country has seen the ready availability of deepfake tools throw oil on an already burning fire. The numbers speak for themselves: between 90 and 96 percent of all deepfake content involving identifiable individuals is non-consensual and sexual in nature, and women account for nearly 99 percent of those affected.

Even so, India's legal framework has struggled to mount an adequate response. The Information Technology Act, 2000[3]; the Bharatiya Nyaya Sanhita, 2023; and the POCSO Act, 2012 all came into existence before generative artificial intelligence became a practical reality, and none were ever intended to address the possibility of manufacturing intimate imagery of people who had no involvement in or awareness of such content. This has left a stark and troubling void between the gravity of the injury being caused and the capacity of the law to meaningfully respond.Second, what changes to law, institutional structures, and processes are needed to build a legal response genuinely capable of addressing AI-generated non-consensual intimate imagery? These core questions are supplemented by enquiries into what can be learned from other jurisdictions, what responsibilities ought to rest with digital platforms, how freedom of expression concerns can be navigated, and how far courts can stretch existing law before legislation becomes unavoidable.

II. UNDERSTANDING THE TECHNOLOGY AND THE HARM

A. Technical Architecture

The three main technologies involved in generating deepfakes involve distinct mechanisms. The first is known as a Generative Adversarial Network [4]orGAN, and was initially proposed by researcher IanGoodfellow and others in 2014. In the GAN model, two different neural networks oppose each other; the first one generates fake images that look real, while the second one checks these generated images and tries to detect whether they are authentic. This back-and-forth process between these networks continues until the image generation network becomes very proficient in its task such that it generates images that cannot even be detected to be fakes

[3] Information Technology (Amendment) Act, 2008

[4] Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., & Bengio, Y. (2014). Generative adversarial nets. In 'Advances in Neural Information Processing Systems' (pp. 2672–2680). Curran Associates, Inc.

 [ISSN 2581-5369]

by experienced professionals. Earlier models of these networks required substantial computational power in order to work, and even then, a large number of source images,sometimes amounting to hundreds, were needed before generating successful results.This was altered by the passage of time and rapid technological development; by 2022, it became possible to generate a convincing deepfake based on just two pictures of the target individual. The second approach, which is based on the use of what are referred to as diffusion models, represents a completely different way to achieve the same end. While training, this sort of software is presented with real images gradually corrupted to the point at which no recognisable picture information is left. In essence, the software learns how to corrupt the image by learning to restore it into a comprehensible format. Once trained, such software can generate totally new intimate photos solely on the basis of a written description, without the need for an actual photograph of the individual portrayed. This creates an interesting legal challenge in terms of applying existing legislation to imagery of this type because, while many laws refer explicitly to taking pictures or films of someone, there is nothing of the sort happening when imagery is generated entirely from text by an algorithm.Voice cloning completes the technological package. This is a technology that enables the unique features of an individual's voice, including his or her accent, rhythm, emotional tone, and voiceprint, to be successfully recreated using machine learning techniques on just a small sample of recorded speech from that particular person. The combination of this audio and artificially generated video footage of that person constitutes a deepfake of breathtaking realism that can even be used live in conversations via video.

B. Typology of Harms

Of the various forms of harm that deepfake technology enables, Non-Consensual Intimate Imagery NCII[5] is both the most common and in many respects the most emblematic. The offence involves using AI software to generate sexually explicit material featuring a real, identifiable individual, with the raw material typically being innocuous photographs sourced from the victim's social media presence. What fundamentally distinguishes this from earlier forms of image-based sexual abuse is that it has severed the last remaining practical obstacle that once limited this kind of victimisation: the perpetrator no longer needs to have obtained any genuine intimate image of the target. The technology itself now performs that role entirely.

A separate but related form of harm emerges when fabricated intimate imagery is turned into a

[5] Cal. Civ. Code § 1708.86 (West 2019) (California, USA) (non-consensual deepfake intimate images – civil remedy).

 [ISSN 2581-5369]

weapon of extortion. Abusers bank on the victim's inability to say with any confidence whether what they are being shown is real or manufactured, presenting synthetic content as though it were genuine compromising footage and threatening to release it unless their demands are met demands that may be monetary, sexual, or both. The psychological grip this exerts on victims can be overwhelming, sustained entirely by the fear and uncertainty that not knowing the truth creates.

Generative AI has also been put to the deeply troubling use of producing child sexual abuse material, and the legal questions this raises under India's POCSO Act are unresolved and cannot wait much longer for answers. The crux of the problem is whether the law's ban on child pornography covers images that are entirely the product of software content conjured without any real child ever having been present, harmed, or photographed. No Indian court has yet squarely addressed this question, and that silence leaves a worrying hole in the legal shield that is supposed to protect children.

At a wider societal level, sexual deepfakes have become a tool of calculated professional destruction, aimed most often at women who have worked hard to build visible and influential careers. Journalists pursuing difficult stories, politicians, activists, and academics have all had fabricated sexual imagery used against them not out of personal grudge, but as a cold and deliberate attempt to destroy their reputations, drive them away from the work they have chosen, and warn other women that public life comes at a price. The damage this does extends far beyond any individual victim; it quietly narrows the space in which women feel safe to lead, speak, and be seen.

C. Victims and Psychological Impact

The evidence on who bears the cost of deepfake sexual exploitation is both extensive and consistent. One large-scale study that examined in excess of 15,000 videos circulating across online platforms established that 96 percent of the material reviewed was non-consensual sexual content, and that women comprised 99 percent of the people depicted within it. The harm sustained by victims extends well beyond reputational damage: documented psychological consequences include debilitating anxiety, severe depression, post-traumatic stress disorder, and suicidal ideation, with the intensity of these outcomes observed to be broadly comparable to those recorded among survivors of physical sexual assault. The Indian context introduces additional layers of vulnerability. Social structures in many parts of the country remain heavily invested in female sexual propriety as a marker of personal and family honour, with the result that the circulation of fabricated sexual imagery irrespective of whether its artificial nature is

 [ISSN 2581-5369]

eventually established can simultaneously destroy a woman's reputation, damage her family's standing, foreclose her professional opportunities, jeopardise her marriage prospects, and in some circumstances place her physical safety at risk.

D. Evidentiary and Jurisdictional Challenges

Confirming the artificial nature of any videos or images before admitting them into evidence would entail enormous costs and efforts. Namely, it would imply recruiting specialists who possess sufficient skills to recognize several factors, which prove the artificiality of the content in question from incorrect eye movements to some anomalies that may be traced only at the pixel level. Unfortunately, India does not have any instruments for performing such a task. The nation has neither a generally accepted methodology for analyzing such materials nor special laboratories or any experience related to recognizing videos or images as synthetic.

The problem becomes even harder when we talk about the cases where the person who suffers is the citizen of the country, while the offenders come from another state. Thus, they would be well-protected by their anonymity, which serves as the first barrier between them and the offended party.

III. INDIA'S CURRENT LEGAL FRAMEWORK AND ITS LIMITATIONS

A. The Information Technology Act, 2000

The Information Technology Act looks like it provides some level of protection against the deepfake sexual exploitation of others, as it forbids the disclosure of any image of another person that shows intimate parts of their body without their consent. But a careful reading of the provision's text shows that there is a real stumbling block in the provision itself. The concept of "capture" clearly references the tangible act of photographing or filming a real person in a real situation is the core of the section. It's not like that with deepfake content: The content is not recorded from real, but created by software based on data inputs. There's no camera trained on the victim. There are not still moments. Whether the algorithmic creation of an image is a proper legal term of "capture" and its basic denotation does not give one much hope for those who might want to say "yes."

The lack of adequacy is even more profound in the context of Sections 67, 67A and 67B of the Act which together, ban the online transmission of obscene materials, sexually explicit material and child sexual abuse images. In this context, prosecutors have turned to these provisions for some success in cases of non-consensual sharing of intimate photos. However, they come with a problem that's not just a technical one, but a fundamental one for their use in deepfake cases.

 [ISSN 2581-5369]

All of these provisions focus the legal investigation on the actual content of the material, and ask this question: is the material obscene? Is it sexual in nature? Is it made on display? All of them ask and the main question in any case of a deep fake is whether the person whose image was imprinted consented to their likeness being portrayed in this way. While the presence of offensive material in the world is harmful, deepfakes for sexual exploitation are harmful because they are created with the intent to violate someone's right to control the representation of their body and their identity. Any provisions that focus merely on the content of the material– and not whether anyone agreed to its production–are simply under-equipped to uphold that right.

B. The Bharatiya Nyaya Sanhita, 2023

The Bharatiya Nyaya Sanhita replaced the Indian Penal Code and has come into force since July 2024, 2023[6] being considered a turning point in Indian criminal laws. It certainly was in many ways. However, the reforms it brought did not feature any offence pertaining to sexual exploitation of minors created specifically for the exploitation that occurs via the use of AI; in fact, when examined with care, the provisions it does contain are poorly suited to the exploitation that occurs via AI. It is not enough to prove a false statement, as the BNS does not place an onus on the complainant to prove that the defendant knew it was false, and it has no focus on sexual dignity or bodily autonomy. When, like in most cases, the perpetrator has gone to great lengths to hide behind a variety of digital masks, these evidentiary demands take on an even greater force. The BNS sections on outraging the modesty of a woman were written with physical interaction in mind, and don't readily apply to behavior that happens at a distance over an artificial image. There is a limited remedy in sextortion situations in which the sender of the image or the content is a synthetic image accompanied by a demand for payment, but no legal basis to take action if there is no threatening element in the production and distribution of the content, only a harmful one. In short, the BNS is a refurbished criminal code, but one that is still based on a pre-digital conception of how harm occurs.

C. The POCSO Act, 2012

This definition of child pornography in the Protection of Children from Sexual Offences Act is very wide and could, on one reading, encompass a digitally created representation of a child in a sexualised context. It actually does, at least in part, and in particular, whether it reaches any images that are entirely artificial, those that show no real child, and that are created without any involvement whatsoever by any child at any stage, it does not say.It does, at least in part, and

[6] Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023 (India) (effective July 1, 2024).

 [ISSN 2581-5369]

at least in particular whether it reaches entirely artificial images, images showing no real child, and produced without the involvement of any child at any stage, does not say. This is not just a minor technicality. The rise in creation of child sexual abuse synthetic content using generative AI and the lack of consensus on the issue as to whether such content is covered by the purview of POCSO could be a significant lacuna in the protections the Act is meant to offer. And added to that is that the victim-centred mechanisms in the Act that identify, help and protect 'real children who have suffered real abuse' have no natural extension to the situation of a completely made-up image with no actual child being identified as the victim or harmed.

D. IT Rules, 2021 and Platform Regulation

The rules that the government made in 2021 for media platforms are mostly based on people complaining. Social media platforms have to do something about content after someone reports it. They do not have to look for content before it hurts people. This is a problem when it comes to fake sexual pictures that can be seen by thousands of people in just a few hours.

The rules do not say anything about keeping evidence. This means social media platforms do not have to save things like account details when something was uploaded and other important information that would be needed if someone wanted to take action. By the time someone decides to go to court the evidence that could help find the person who did something might be gone.

The punishment for media platforms that do not follow the rules is not strong enough.There seems to be an absence of any form of punishment because it has been thought that it would not be sufficient enough for the social media site to fulfill its responsibility effectively. The social media site should make sure that the offensive content will never be found on their platform as well as having enough proof against the person guilty of committing the offense.

E. Constitutional Right to Privacy

This verdict was delivered by the Supreme Court in the case of Justice K.S. Puttaswamy vs. Union of India[7] in the year 2017. It is pertinent to note that the present issue has nothing to do with the problem of modifying images using artificial intelligence. But this verdict assumes tremendous importance while considering the legal aspects of the regulations for deepfake manipulation. As per the Supreme Court's judgment, there is a right to privacy in Article 21 of the Constitution.This decision gives us a reason to make changes to the laws as we will talk about in this paper. We can already see the effect of this decision in the rulings of the High

[7] Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1

 [ISSN 2581-5369]

Court in cases where technology is used to harass people or share private content without permission.. We need to be realistic about what this decision can do. The fundamental rights in the Indian Constitution are mainly to protect us from the government doing something. These rights do not automatically make it a crime for individuals or companies to do something wrong.

The decision in Justice K.S. The Puttaswamy v. Union of India case shows us that we need to make some changes and that these changes are allowed by the Constitution. However this decision alone cannot make these changes happen. We need the government to make new laws for that to happen. The Justice K.S. Puttaswamy, v. Union of India decision is important. It is just the start. We need to take steps to really make a difference.

F. Summary of Gaps

A systematic review of India's existing legal framework in light of the harms described above yields a picture of comprehensive inadequacy organised around six identifiable structural failings. The most glaring is the complete absence of any dedicated criminal provision targeting the production or dissemination of non-consensual synthetic intimate imagery; those seeking legal redress are forced to press their cases under laws designed for entirely different purposes. Closely related is the second failing: the conceptual framework underpinning the most potentially applicable provisions is built around obscenity rather than consent, meaning that the legal wrong these laws recognise is categorically different from the harm that deepfake sexual exploitation actually inflicts. Third, the provisions that come closest to addressing image-based abuse most notably Section 66E rest on assumptions about the physical recording of real images that make them structurally inapplicable to content generated by algorithms. Fourth, even in those cases where existing law can be made to apply through creative interpretation, the penalties available bear no meaningful relationship to the severity, permanence, and breadth of harm that deepfake exploitation causes. Fifth, the regulatory architecture governing digital platforms is reactive, inconsistently enforced, and stripped of any obligation to preserve the evidence that victims need to pursue justice. Sixth and finally, the legal system as currently constituted offers victims no procedural protections of any kind, no automatic anonymity, no guaranteed evidence preservation, no expedited pathways to relief meaning that engaging with it often compounds rather than alleviates the harm already suffered.

 [ISSN 2581-5369]

IV. COMPARATIVE LEGAL ANALYSIS

A. United Kingdom

The most significant measures in the Online Safety Act 2023[8] and the changes to the Sexual Offences Act are outlined below.The most complete architecture of the jurisdictions studied. The Sexual Offences Act has now been replaced.Outlaws the production and sharing of non-consensual photographs, images and videos of intimate images Synthetic imagery on a voluntary basis, regardless of obscenity. The Safety of Children Online Act.[9] makes proactive obligations to the platform with high financial fines for non-compliance. The main takeaway from the UK framework is the reorientation from obscenity to the following: A paradigm shift from paradigm to consent paradigm.

B. United States

Though there have been numerous efforts in Congress, including a bill, no federal legislation has been passed, DEEPFAKES Accountability Act. State legislation (California, Texas, Virginia[10]) is applied to fill the gap. part of the gap. The US experience teaches two lessons: the importance of statutory civil remedies and the need for increased focus on the advantages of these remedies. with damages without proof of financial losses; and the risks of legislative

India's national criminal law system is structurally predisposed to fragmentation, which poses a threat.

C. South Korea

Amendment to the Act on Special Cases Concerning the Punishment of Sexual Crimes, criminalise both production and distribution of content by the "nth Room" scandal non-consensual synthetic intimate images. In South Korea[11] the contributions are: keeping production independent from distribution; and showing that the commitment of institutions to the enforcement of legislative reform is necessary for it to work.effective.

D. European Union

AI-generated content that is provided as labels must be disclosed in accordance with the EU AI Act (2024).[12] The Digital Services Act demands large platforms to carry out systemic risk assessments and implement measures. structural risk-mitigation measures. The EU model

[8] Online Safety Act 2023 (UK)
[9] Sexual Offences Act 2003 (UK) as amended by Online Safety Act 2023
[10] California Civil Code, s 1708.86 (USA)
[11] Act on Special Cases Concerning the Punishment of Sexual Crimes (South Korea) as amended 2020, Art 14
[12] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 on Artificial Intelligence (AI Act) [2024] OJ L 1689/1

 [ISSN 2581-5369]

illustrates disclosure requirements as: and risk-based regulatory frameworks do not replace criminal law, The obligations that are placed on that platform do not just go to the extent of removing harm, but to the extent of trying to prevent harm**.**

E. Transferable Principles

Six transferable principles emerge: (i) consent as the operative legal standard; (ii) criminalisation of production as well as distribution; (iii) proactive platform obligations; (iv) parallel civil and criminal remedies; (v) penalties calibrated to harm severity; and (vi) victim support infrastructure as a prerequisite for effective law.

V. JUDICIAL RESPONSE AND CASE LAW

A. The Rashmika Mandanna and Alia Bhatt Incidents

The flaws in the current legal system were starkly brought to the fore and discomforted the public with two incidents involving famous personalities from the Indian film industry.

The poseur video, which had the face of actor Rashmika Mandanna[13] merged with another woman's body, surged in popularity in Indian social media feeds in November 2023. The Delhi Police filed a First Information Report, but the investigators soon hit a roadblock: Indian law doesn't have anything special or directly aimed at the creation or sharing of deepfake content, and they had to assemble charges from laws made for different scenarios that fit this case just as much as they were supposed to. All the matter never got to a point where any court had to determine the deepfake liability and the law remained as murky as ever post-crowd.

Soon after, Alia Bhatt's[14] The name was used to create sexist AI-generated images that started circulating on the same sites.The same sites were soon flooded with images depicting actress Alia Bhatt in sexually explicit poses, which were also AI-generated. In some ways this second case was even more telling than the first. It exposed the fact that having an effective legal remedy was not a financial or celebrity or the best lawyers' problem. Even with all the tools at his disposal, a man of luck would come out of the fight with no satisfactory response from the law from what had been done to her.

The two cases together forced an official reckoning with the fact that the legislative vacuum was not imaginary, but real, serious and much needed, and led to a debate in the Parliament on the need for legislation aimed at addressing this harm.

[13] Sharma, A. (2023, November). Delhi Police registers FIR over viral Rashmika Mandanna deepfake video. 'The Hindu'.
[14] Alia Bhatt deepfake video goes viral for the second time this year, sparks outrage By 'The Hindu'

 [ISSN 2581-5369]

B. Morphed Image Jurisprudence

While deepfake technology is relatively new, the problem of genuine photos being used to place people in compromising positions, that is, in situations that they did not pose for was already a big issue in Indian courts. High Courts in a few decisions interpreted the provisions of Section 66E and 67A of the Information Technology Act in a manner that would cover morphed images. This body of jurisprudence is important because it shows that the Indian judiciary will read the existing statutory provisions in a liberal manner, and when it is faced with technological harms that Parliament did not explicitly foresee. However, blindly copying and applying existing law to morphed images is not an effective solution to address fully synthetic deepfake content. Often, the two types of harm look alike yet underneath they are very different and in an important way different legally: in every morphed image case there is an actual photograph of the victim, and the manipulated content is based on that photograph. The court is always presented with an image that, at its heart, is of a real person in a real moment. With a diffusion model deepfake, no such underlying photo exists. No photos of the victim ever were taken; no pictures of her were ever taken. The material was all created by computer and the so-called "protected" provisions of the court that have been expanded to fit morphed images don't have any parallel in that context.

C. Constitutional Privacy Jurisprudence and Judicial Limits

Such constitutional values, as expressed in the Puttaswamy judgment, are reflected in various High Court rulings on issues of sexual harassment using technology and the sharing of personal images without consent. Judges have been applying these considerations to other legislation which may have been construed differently, and have done so with a pro-victim attitude, and this is a welcome development. However, there is a constitutional limit which even the most creative and sympathetic judicial interpretation cannot go over. Legality is one of the fundamental principles of any rule-of-law system, which states that nobody can be convicted of a criminal offence if it had not been specifically described by law at the time the act was committed. They can interpret ambiguous language liberally, courts may make analogies from similar situations, and they build up the common law over time but they cannot create a criminal offence out of thin air where the legislature did not. This is not a lack of judicial will, it is a realization of the right lines of demarcation between the two powers. The constraint is especially meaningful in the current setting because Indian courts have not been averse to the recognition of this constraint in an explicit manner. In a few judgments relevant to the issue of technology facilitated abuse, the court has commented not only on the injustice of the facts before it, but also on the lack of adequate statutory provisions to address the situation and urged Parliament

 [ISSN 2581-5369]

to fill this gap with a specific legislation. These judicial statements, from many different jurisdictions and over several years, provide as clear an institutional endorsement for the necessity for legislation as the constitutional order allows courts to provide.

VI. PROPOSED LEGAL REFORMS

The criminalisation of non-consensual distribution of intimate images of actual persons created by artificial means is more basic and more necessary of the legislative changes this paper recommends than any other. Otherwise, all the proposals for reform in this document come to little. The conceptual bed rock of the new offence is consent; that is, whether or not the person whose image was appropriated had authorised what was done with it, and it is a question that has to be asked directly and morally simply, that is.The conceptual cornerstone is the presence or absence of consent, which asks a direct and morally coherent question: did the person whose image has been appropriated authorise it? This is a different question than the one being asked in India by the provisions based on obscenity, which focuses on the contentiveness of the content and not on the rights of the person depicted in it. The offence should apply to any image, video or audiovisual recording that has been generated or materially altered using artificial intelligence, which shows a recognisable real person in sexual situations, or in a state of nudity, but which was done without the real person's true consent. Equally importantly, this law should clarify that this consent doesn't only require that someone is willing to let it be printed, nor is it just the fact that someone's photos are online. Consent must be freely and voluntarily given, relate specifically to the use in question, be based on a proper understanding of what is being agreed to, and be susceptible to withdrawal by the individual at any time if he or she chooses. If a person chooses to use social media, to display photographs of themselves publicly, or to appear in any media which is publicly accessible, then such choices should be made explicit in the law so they do not mean that the person consents to the creation of synthetic intimate material.

The law should cater for aggravated forms of the crime and impose a more severe maximum punishment for those aspects of the misbehaviour which are particularly serious. The circumstances surrounding the treatment of such a person should involve the targeting of a victim who is a minor; exploitation of the position of trust or authority that the perpetrator held in relation to the victim; the production of the material for commercial purposes or for financial gain; and the dissemination of the material to many people or on multiple platforms. This progressive approach recognises that deepfake sexual exploitation can vary significantly in its seriousness and that the response to the offence should reflect this. In terms of sentencing, the

 [ISSN 2581-5369]

current maximum sentence of three years imprisonment provided by Section 66E of the Information Technology Act[15] is highly inconsistent with the harm that deepfakes bring to the exploited and the long-term damage they cause in the lives of women and children. A new punishment system should be agreed and adopted, which would have a cap of seven years imprisonment for the typical offence, and be increased to ten years if the aggravating factors outlined above apply in a broadly similar manner and are commensurate with the nature of the injury incurred and its lasting nature.

A. Civil Remedies

While the criminal law is essential, it is not sufficient to provide victims of deepfake sexual exploitation with sufficient redress. Criminal prosecution is a process that is at the discretion of the state, not the victim, and depends on the identification of one or more perpetrators, and the imposition of punishment without providing tangible or direct relief to the individual who suffered the harm. In many instances involving deepfakes these challenges are especially significant: perpetrators often use technical methods to hide their identity, may be based in countries outside of the jurisdiction of Indian law enforcement, or may not be identified at all. For any wide-ranging legal response, it is important to include the possibility of a direct civil remedy, outside any criminal process, which is available to the victim to act for themselves. This remedy should be patterned after that which is provided in California where victims have a right to statutory damages, where no specific financial loss need be identified, quantified and proven, but where amounts are set by statute. This is essential as the most severe effects of deepfakes exploitation, mental anguish, damage to reputation, loss of personal dignity cannot be easily quantified. If the evidence reveals the perpetrator intended to inflict intentional harm or deliberate or calculated cruelty, then the court should have the ability to impose a higher damages level than the statutory minimum. Preliminary injunctive relief needs to be granted in an urgent manner, allowing courts to remove harmful material before a proper hearing only for every hour it is available, to be an extension and intensification of the harm that just occurred. Winners of civil cases should also be entitled to benefits for the cost of action they had to take, in order to avoid making it more difficult for the victim to experience the justice they deserve because of the financial burden of bringing the case to court.

B. Platform Accountability

The model of platform regulation that is currently contained within the IT Rules in India is fundamentally misaligned as it imposes obligations on platforms only after a complaint has

[15] Information Technology Act, 2000 (Act No. 21 of 2000)

 [ISSN 2581-5369]

been received and reported, and the spread of such deepfake sexual content and how it causes harm. Harmful synthetic imagery does not stand around waiting expectantly for its discovery and reporting; it moves through networks like a bullet, gaining traction and reaching large audiences in hours of its upload. Often when a victim learns that such content exists, affects the reporting process on the platform, and waits for a response, it is in many cases too late and irreparable harm has already been inflicted. Reform needs to therefore go from reactive to anticipatory with the fundamental nature of platform obligations. There should be a legal requirement on large social media intermediaries and content hosting platforms that must invest and ensure the availability of technological mechanisms that can detect the creation of synthetic intimate images and block such images before they become widely circulated, and such technological mechanisms must be updated as the technology to create such images evolves. Removal of harmful content should be required within a specific timeframe, preferably 24 hours, and even more strictly in the case of content depicting persons under the age of 18, after harmful content has been reported. Once a complaint is received, there should be an automatic, non-negotiable obligation to maintain all electronic evidence relating to the reported content including account information, upload histories, device identification, metadata, etc., for a duration that is adequate for any investigation or litigation that may arise. It should be mandatory to report regularly and in detail to a specific regulatory entity the number of complaints received, the response time reached and the conclusions of each complaint, establishing an open and transparent evaluation record of the performance of the platforms. If platforms are not fulfilling these obligations, the financial penalties that may be imposed must be sufficiently severe to incentivize genuine compliance: penalties should be tied to the global revenues of the platform, so that even its largest and most commercially powerful platforms would not be able to afford not to comply.

C. Procedural and Institutional Reforms

As is often the case in the history of legal reform, good laws that are poorly implemented result in minimal impact on the ground. In the particular case of deepfake sexual exploitation, it is essential to have a parallel programme of institutional development to back the legislative changes proposed above. Specific investigation units should be created in the cybercrime division of state police forces, with officers undergoing tough and continuous training in AI forensics to assist them in analysing AI-generated content, verifying or contesting synthetic origin claims, collecting and preserving digital evidence, and tracking down AI offenders who are sophisticated enough to cover their tracks. But it is not only the investigators who need structured training programmes to ensure that they are sufficiently knowledgeable about the

 [ISSN 2581-5369]

technology to perform their function competently and fairly before a prosecutor who will be required to present complex technical evidence to court, and a judge who will be asked to consider and evaluate it. The attention of the court to the treatment of the victim in the proceedings is a very special and urgent matter. The current system does not guarantee the anonymity of a victim of deepfake SEx: the information and data relating to their situation could be disclosed in court documents, judgements published or in media coverage, thus subjecting the victim to exactly the kind of exposure that the perpetrator is looking for and that the victim is trying to escape. This exposure often acts as an unbridgeable barrier to reporting and simply does not work for the very people it is meant to serve. Statutory anonymity, therefore, should be guaranteed from the initial complaint, automatically and unconditionally, and should be extended without any restrictions to any criminal, civil and regulatory proceeding stemming from the same facts. If it is the victims' most urgent request that harmful content be removed from circulation as quickly as possible, dedicated fast-track procedures, which have been trained to carry out the orders, should be in place before courts that have the technical expertise to do so, and that will be able to issue binding orders within days instead of months. A statutory national regulatory body with legitimate and effective powers to oversee platform compliance, to accept and consider victim complaints from all over the country, to investigate systemic failures and to coordinate enforcement activity between the central and national authorities should be established.

D. Reform Roadmap

The scope and ambition of the reforms outlined in this section is fully recognised. This will take time, involve ongoing political buy-in and necessitate the concerted action of legislative, executive and judicial institutions to see this become a reality. A staged process of implementation in three time horizons is the most realistic means to take the current situation of inadequate progress towards a full-fledged framework, starting from the perspective of those victims of deepfake sexual exploitation.

The most urgent reforms that must be implemented in the next year focus on the most effective, and most easily possible, aspects of the reform agenda. Without the consent-based criminal offence, the rest of the existing legal system is either ineffective for victims or does not function at all, and making it does precede the ability to do many of the other things that follow. At the same time, the statutory provisions for victim anonymity must be implemented, taking away one of the most effective practical barriers to reporting. The IT Rules should be urgently amended so that they include the 24-hour takedown requirement and automatic evidence preservation, providing immediate improvements to the existing regulation of platforms.

 [ISSN 2581-5369]

The medium term reform programme (2-3 years) should aim at making the general programme more concrete. This phase involves establishing the statutory civil remedy and its associated statutory damages mechanism, forming and equipping specialist deepfake investigative teams in state cybercrime units, drafting and implementing training materials for prosecutors and courts that can offer a real deterrent to non-compliance for the existing platform penalty regime, and establishing a revenue-proportionate sanctions system that can function as a meaningful deterrent to non-compliance.

The longer-term agenda, over the next five years, covers the system and international aspects of the issue and will need more persistent efforts to resolve. This stage should include the development of a dedicated national regulatory framework with all its statutory powers, the integration of a comprehensive digital education curriculum across all levels that provides robust substantive education on synthetic media, consent and legal rights and remedies, and the active seeking of bilateral and multilateral international agreements to enable international evidence sharing, mutual legal assistance, and coordinated enforcement action against cross-border deepfakes offences.

VII. ADDRESSING COUNTER-ARGUMENTS

Freedom of Expression

The fear that a criminal offence on deep fakes sexual content will be overbroad and that it will inadvertently have a chilling effect on lawful expression of creative or political speech is misplaced because the proposed offence doesn't target creative or political speech. This proposed bill does not seek to target expression as it is normally understood. It is focused on the production and dissemination of sexual images of identifiable real persons, where the person's sexuality is not the aim of the image, but the object of a deliberate violation of bodily autonomy and sexual dignity of another person without their consent. There's really no well-established theory of free expression that would recognize the unconsented production of fake pornographic imagery of a real person as speech that ought to be protected by the Constitution. Where there is a genuine uncertainty at the margins, for example in the case of content created for journalistic, political, satirical or artistic purposes and which may reasonably be said to touch on such content, then this uncertainty is adequately addressed by ensuring the legislation is explicitly drafted to include such content where it is created for these purposes. In its Puttaswamy judgment, the Supreme Court has dealt with the deeper constitutional question about how the freedom of expression guaranteed in Article 19(1)(a) of the Constitution[16] is to

[16] Article 19 Of The Indian Constitution: A Comprehensive Analysis.'Mondaq.com'

 [ISSN 2581-5369]

be balanced with the right to privacy guaranteed in Article 21. The decision held that privacy, in that instance the right's aspect with regard to sexual autonomy and the right of an individual to control how his or her body and identity are represented, is a sufficiently weighty and compelling constitutional interest to warrant the imposition of proportionate restrictions on expressive conduct that infringes on it without consent. The proposed crime fits very neatly into the zone that the Constitution thereby affords for legislation.

The Detection-Generation Arms Race

One of the many arguments against deepfake laws is the technological aspect of enforcement: generation technology, the argument goes, that it outpaces detection by a mile; It is important to note that this does not require anyone to prove as a prerequisite for a legal regime that particular content is suitable for children under 14. The target of synthetic will be continually slipping away and will often not be able to capture.The proof required in order to prove responsibility. This is a valid observation in terms of it being technically accurate.Should not be taken lightly. It is not, however, a law with the same mandate as its.

Those who support it say they attribute it to. Most of the harmful deepfake sexual content in practice is not created with advanced and sophisticated generation systems at all.Designed to resist forensic analysis, it is made with readily available commercial materials.

Applications and open source tools which are much less technically advanced and which leave The presence of algorithmic traces in their outputs that can be identified. The vacuous case of the idealized balancing of the idealized.The empty case of the empty balancing of the empty.

One cannot technically prevent a deep fake, but it is not the case that law enforcement could not prevent it.Most of the scenarios that enforcement will encounter are ones that are similar to these. In addition, it is important to note that forensic evidence is of great value.However, device forensics is not the only evidentiary pathway that is available to the prosecutor: The witness testimony, record of accounts and circumstantial evidence may all contribute to determining liability without a clear technical decision of whether or not the liability exists. A specific image is real or fabricated. Most importantly, perhaps, the argument of an arms race. is a positive affirmation of the need for mandatory pre-publication detection obligations on platforms. Should the post-hoc detection challenge prove to be a true challenge, supports the case against releasing unsavoury material.Available data, identified the need for the new model.The new model was distributed at precisely the moment that the platform's own detection instruments, based on data available, determined the need for the new model. Unoptimised content has the best chance of being identified.

 [ISSN 2581-5369]

Enforcement Realities

A related and somewhat different objection argues that any new laws in this realm would be pointless. Given the present condition of law enforcement and judicial institutions in India, on any given day, any of these can be overcome as there is a lack of specialized equipment to conduct the proper evaluation of the incident, specialist personnel, and forensic infrastructure to properly evaluate the incident. A framework for investigating and prosecuting deepfake offences is necessary, along with the effective procedural frameworks. When regulatory bodies are lacking the capability to carry out their duties,according to the argument, new laws will yield nothing more than false hope for victims and empty threats to perpetrators. This objection is legitimate. In the event of a clear achievement gap between.The solution to legislative ambition and institutional capacity is to tackle both at once to pass the Develop a sound legal structure and invest in strengthening enforcement capacity for the effective implementation of the law.give it effect. It is certainly not a step that should be taken to kick the can down the road until institutions have had time to consider policies, programs, and products.came up with the idea to self-impose laws that were not yet established. This pattern of the development of law and institutions running side by side, each supporting the other is now, exactly how effective regulatory regimes have been created in comparable fields, from financial From local crime to environmental control to cybercrime in general. The institutional reforms A specialist investigative unit, designed under the proposals in the previous section of this paper, will be targeted at the training of specialists for the investigation of offences. For prosecutors and judges, dedicated regulatory oversight are designed expressly to close the objection that recognises a capacity gap this, they are envisioned as parts of an This is an integrated reform package as opposed to aspirational additional reforms that could be worked for at some point.unspecified future point.

Risk of Over-Criminalisation

A third line of objection is that the proposed offence is too open-ended and may be able to capture within the criminal law conduct that may not truly be deserving whether by criminalization of private conduct which does not directly affect others or by the criminalization of collective action aimed at social reform. others, by providing opportunities for the false or malicious accusations of: It is hard to defend against, or criminal penalties, in cases where less extreme or other civil remedies would be sufficient and appropriate.

The risk of inappropriate criminalisation of purely private Primary offence is structured around the act of distribution or a Where there is a clearly expressed intention to distribute, and not just

 [ISSN 2581-5369]

to create in isolation:private, synthetic production of images of private intimacy which do not leave the perpetrator. possession and it is never shared with anyone does not lead to criminal liability under the proposed framework. The worry is about false accusations taking advantage of an easily manipulated All principles of criminal liability in all civilised countries are taken as a basis for offence. context: the prosecution has to prove its case to the degree of beyond reasonable doubt, The accused is presumed innocent until that standard is met, and the courts have full authority to.Analyze evidence carefully and appropriately. There is no compelling evidence to consider deepfakes are uniquely vulnerable to invented claims, and which is why there is a significant chance these will proliferate in the future.That is why deepfakes could be prone to fake claims hence their potential to be widespread in the future.Distinguishes them from other serious sexual offences, which have always been subject to the same objection and have been handled in the same evidentiary context.

Make sure that the criminal law's response is matched with the seriousness of the conduct in each individual case. In the first place, and in light of the alternative or additional remedy of civil action. Excessive or impractical criminal prosecution: avenue. The overarching principle is one of proportionality but proportionality, properly understood, must be met with legal action that is in proportion to the harm done, and the harm done by The full force of the criminal law should be applied to deepfake sexual exploitation.

VIII. Conclusion

The conclusions drawn from the various parts of this paper indicate that the current laws in India are not only inadequate in addressing cases of deepfake sexual exploitation but also are structurally unfit to deal with such cases. The failure is not one which can be overcome by clever interpretation by the judges or by the ability to simply reinterpret existing provisions to fit into situations that the drafters did not anticipate. It's more than that. The existing laws protecting victims were created in an era of technology that was vastly different and were conceived based on the conceptual framework of obscenity, and designed to react to the harm after it has been reported, and not to curtail the spread of harm in the first place. A lack of a legal framework that is commensurate with the immoral violation being remediated will be uncompensated by the good will of investigators, prosecutors, or judges.

The central issue of the paper is a normative one which must be clearly and unequivocally stated. While digital content control and platform management are aspects of the issue, deepfake sexual exploitation is fundamentally an issue of power.Deepfake sexual exploitation is about power, rather than digital content control or platform management, although there are aspects

 [ISSN 2581-5369]

of control and management of digital content that affect deepfake sexual exploitation. It's, on a fundamental level, a type of gender-based violence. It was designed with women in mind, it is used consistently against womenand not just randomlyat a rate that would seem almost as if it were designed that wayand it is very damaging to the psychological, professional and social well-being of those who are targeted by it, as research has revealed it to be broadly comparable to the outcomes of physical sexual assault. A legal framework based on the false notion that this is an ancillary issue of a larger content-moderation issue has made a category error; it's taken the wrong approach to solving the problem, as well as the wrong problem. It's not just a drafting preference, but also an understanding of what the abuse is really about and toward whom it is really directed.

To end this paper in a purely critical mood and without noting the positive aspects that have been noted here, however, would be a counsel of despair. India has the means necessary to face this challenge with a positive response. This paper proposes the reforms based on the constitutional principles laid down by the Supreme Court in Puttaswamy[17], wherein privacy is recognised as a fundamental right, and the scope of privacy is interpreted to include bodily integrity and personal image control, which gives the legislators the normative justification and the constitutional authority to make them. These are the two other processes criminal law reform, with the enactment of the Bharatiya Nyaya Sanhita,[18] and the reform of the regulation of digital devices, which is ongoing under the Digital India Act, which is currently in draft of which these are just two examples; other changes could be made through the existing laws and procedures of these two areas of reform, rather than by developing a new legal system from scratch. Existing experience in the UK, South Korea, the USA and the EU shows that it is possible to successfully implement legally responsive measures against deepfake sexual exploitation, and provides clarity on the design considerations for constructing such measures.

India lacks the constitutional powers, not the opportunity to legislate, not the opportunity to emulate powerfully. What it needs and what no amount of academic research can replace is the political will to see that the systematic violation of women by AI is the serious, urgent problem that it clearly is and take action on that recognition before it becomes so entrenched and so easily accessible that it becomes the unchallengeable reality of women's life in the digital age. Each day the legislative gap outlined in this paper persists, it is a day in which real women can be depicted in sexual ways and images disseminated in India with no liability. The women who

[17] Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1
[18] Bharatiya Nagarik Suraksha Sanhita, 2023

 [ISSN 2581-5369]

are the predominant victims of this technology have already waited long enough.

*****

 [ISSN 2581-5369]

IX. REFERENCES

Indian Legislation

1. Constitution of India, 1950
2. Information Technology Act, 2000 (Act No. 21 of 2000)
3. Information Technology (Amendment) Act, 2008
4. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021
5. Bharatiya Nyaya Sanhita, 2023 (Act No. 45 of 2023)
6. Bharatiya Nagarik Suraksha Sanhita, 2023 (Act No. 46 of 2023)
7. Protection of Children from Sexual Offences Act, 2012 (Act No. 32 of 2012)
8. Protection of Children from Sexual Offences (Amendment) Act, 2019

Foreign Legislation

1. Online Safety Act 2023 (UK)
2. Sexual Offences Act 2003 (UK) as amended by Online Safety Act 2023
3. DEEPFAKES Accountability Act, H.R. 4355, 116th Congress (USA, 2019)
4. California Civil Code, s 1708.86 (USA)
5. Texas Penal Code, s 21.165 (USA)
6. Virginia Code Annotated, s 18.2-386.2 (USA)
7. Act on Special Cases Concerning the Punishment of Sexual Crimes (South Korea) as amended 2020, Art 14
8. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 on Artificial Intelligence (AI Act) [2024] OJ L 1689/1
9. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act) [2022] OJ L 277/
10. Budapest Convention on Cybercrime (Council of Europe, ETS No. 185, 2001)

Indian Case Laws

1. Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1
2. Shreya Singhal v. Union of India (2015) 5 SCC 1
3. Aveek Sarkar v. State of West Bengal (2014) 4 SCC 257
4. S. Rangarajan v. P. Jagjivan Ram (1989) 2 SCC 574
5. Ranjit D. Udeshi v. State of Maharashtra AIR 1965 SC 881
6. Avnish Bajaj v. State (NCT of Delhi) (2005) 116 DLT 427

 [ISSN 2581-5369]

Parliamentary and Government Documents — India

1. Ministry of Electronics and Information Technology, Advisory to Intermediaries and Social Media Platforms Regarding Deepfakes (MeitY, 7 November 2023)
2. Ministry of Electronics and Information Technology, Consultation Paper on the Digital India Act (MeitY, 2023)
3. Ministry of Electronics and Information Technology, Annual Report 2022–23 (MeitY, 2023)
4. Standing Committee on Information Technology, Safeguarding Citizens Rights and Prevention of Misuse of Social and Online News Media Platforms Including Special Emphasis on Women Security in the Digital Space (Lok Sabha Secretariat, Twenty Second Report, 2022)
5. Lok Sabha Debates, Unstarred Question No. 1423: Deepfake Technology and Regulation (Winter Session, December 2023)
6. Indian Cyber Crime Coordination Centre, Annual Report 2022–23 (I4C, Ministry of Home Affairs, 2023)
7. Law Commission of India, Report No. 289 on the Bharatiya Nagarik Suraksha Sanhita, 2023 (Law Commission of India, 2023)

Foreign Government and Institutional Documents

1. European Commission, Proposal for a Directive on Combating Violence Against Women and Domestic Violence, COM(2022) 105 final
2. European Union Agency for Fundamental Rights, Violence Against Women: An EU-Wide Survey (FRA, 2014)

Books

1. Citron, D.K., Hate Crimes in Cyberspace (Harvard University Press, 2014)
2. Henry, N., McGlynn, C., Flynn, A., Johnson, K., Powell, A. and Scott, A.J., Image-Based Sexual Abuse: A Study on the Causes and Consequences of Non-Consensual Nude or Sexual Imagery (Routledge, 2021)
3. Husak, D., Overcriminalization: The Limits of the Criminal Law (Oxford University Press, 2008)
4. Duff, R.A., Answering for Crime: Responsibility and Liability in the Criminal Law (Hart Publishing, 2007)

*****

 [ISSN 2581-5369]