
A DOCTRINAL AND COMPARATIVE INQUIRY INTO DIGITAL DIGNITY AND SYNTHETIC CONSENT IN THE AGE OF AI

Devyani Rastogi, O.P. Jindal Global University, Jindal Global Law School

ABSTRACT

The rise of new generative artificial intelligence tools have created a new and troubling form of sexual violence in the form of deepfake and AI generated synthetic sexual imagery, also known as DSSI. By using softwares like Stable Diffusion and undress.app, offenders create hyper realistic pornographic content from ordinary photos of real people, mostly targeting women and children, without their knowledge or consent.

This paper examines *Whether India's current laws and constitutional protections are sufficient to address this unique type of digital sexual violence?*

It relies on the ideas of *Danielle Keats Citron* regarding sexual privacy, *Stefano Rodotà's* concept of informational self determination, and the analysis of deepfakes and free speech by *Mary Anne Franks and Ari Ezra Waldman*.

This paper also demonstrates how DSSI violates the constitutional rights to dignity, bodily autonomy, and moral agency under Articles 14, 19, and 21 of the Indian Constitution.

It also analyses various Indian laws such as:

1. The Bharatiya Nyaya Sanhita 2023
2. The Information Technology Act 2000
3. The Digital Personal Data Protection Act 2023
4. The POCSO Act 2012
5. The Indecent Representation of Women Act 1986.

These demonstrated how the Indian legal system fragmented and inadequate in identifying and addressing this new form of sexual offence.

This paper also drew comparisons from the United Kingdom, South Korea, and the European Union's legal systems and suggests that Deepfake and Synthetic Media Regulation Clause should be included in the current legal system, specifically in the BNS, by recognising the doctrine of synthetic consent as a new legal category with defined legal elements and intent, and implementing a statutory framework for algorithmic accountability.

Introduction

The convergence of generative artificial intelligence and digital sexual violence has led to what scholars describe as the second wave of technology facilitated gender based abuse.¹

Unlike the non consensual distribution of authentic intimate imagery commonly known as revenge pornography, deepfakes and AI generated synthetic sexual images does not require the existence of any prior intimate act at all. A perpetrator requires nothing more than a publicly available photograph and a software like Stable Diffusion and within minutes it creates hyper realistic sexually explicit content depicting the victim in acts that they have never actually performed and to which they have never consented.

Scholars like *Chesney and Citron* described this capacity for frictionless fabrication as a fundamental gap in the relationship between image, identity, and truth.² A 2023 report by Home Security Heroes found that there has been a 550% increase in deepfake pornographic content since 2019 and 98% of all DSSI consisted of unconsensual pornographic material and 99% of identified victims were women.³

India is specifically in danger because with over 900 million internet users and a digital literacy ecosystem that dramatically grown faster than its regulatory system faces acute vulnerability to this new form of sexual offence.⁴

The UN Women Report on Technology Facilitated Gender Based Violence recognises that the algorithmic sexualisation of women constitutes a distinct and escalating global crisis that

¹ C. McGlynn and E. Rackley, 'Image-Based Sexual Abuse' (2017) 37(3) OJLS 534, 536.

² Robert Chesney and Danielle Keats Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2019) 107 California Law Review 1753, 1758

³ Home Security Heroes, '2023 State of Deepfakes: Realities, Threats, and Impact' (2023).

⁴ Telecom Regulatory Authority of India, *Recommendations on Internet Speed, Connectivity and Digital Inclusion* (TRAI, 2023).]

requires urgent intervention by the states and the internal community as a whole.⁵

The legal issues posed by DSSI is not merely technical but deeply constitutional and jurisprudential at its core. When a woman's image is algorithmically sexualised without her consent, her various fundamental rights are violated at once. For example, her right to dignity and privacy under Article 21, her right to informational self determination as stated by *Rodotà*⁶ and recognised by the Supreme Court of India in the case of *Justice K.S. Puttaswamy v. Union of India* and her right to equality before the law under Article 14 of the Indian Constitution.⁷

In cases where the victims are minors, the imagery amounts to synthetic child sexual abuse material or CSAM due to which the obligations of India under the Convention on the Rights of the Child 1989 and the POCSO Act 2012 directly come into play.

This paper proceeds in six substantive parts. Part II analyses India's existing legal framework and identifies its doctrinal gaps through close statutory analysis. Part III examines the constitutional dimensions of DSSI. Part IV develops the doctrine of synthetic consent and also lays down how it would operate in practice. Part V undertakes comparative analysis linking international models directly to proposed Indian reforms. Part VI sets out concrete legislative proposals. A concluding section draws the arguments together.

Methodology

This research paper uses a doctrinal legal research methodology that includes a systematic analysis of primary legal sources like the legal statutes, constitutional provisions, and judicial precedents read against the secondary academic literature and comparative factual data. This doctrinal approach fits this study because the central claim is a legal one and it also contends that the current Indian existing normative framework is constitutionally and legislatively inadequate to address DSSI and a specific reform agenda is needed to address this adequately

The comparative framework is purposive, not descriptive. The United Kingdom, South Korea and the EU are not merely analysed as templates to be copied. Instead, all of them are analysed because they highlight where the current Indian framework lacks and what legislative options

⁵ UN Women, *Technology-Facilitated Gender-Based Violence: Making All Spaces Safe.* (UN Women Policy Paper, 2022).]

⁶ Stefano Rodotà, 'Data Protection as a Fundamental Right' in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer 2009).

⁷ Justice KS Puttaswamy (Retd) v Union of India (2017) 10 SCC 1.

are the most feasible to us.

The UK matters because it has a common law comparator with a recently enacted specific offence. South Korea offers a civil law Asian comparator that built its legal response in the direct light of the documented mass victimisation. On the other hand, the EU provides a supranational regulatory model that addresses both platform accountability and the broader governance of AI systems.

The theoretical framework is pluralist and it draws its arguments from feminist legal theory of McGlynn, Rackley, Fanks and Waldman, privacy scholarship by Citron, Solove and Allen and the idea of informational self determination given by Rodota to build a foundation for the doctrine of synthetic consent.

Two main limitations of this paper are:

- The paper relies completely on sources which are primarily available only in English language which limits its engagement.
- A significant bridge continues to exist between the proposed legal reforms and the practical realities of the enforcement of criminal laws in India.

The Existing Indian Legal Framework and its Legal gaps

The BNS, 2023 which replaced the IPC, 1860, provided a real opportunity for the Indian criminal system to include digital crimes within its ambit. However, that opportunity has not been taken as of now.

A close reading of the BNS highlights that the framework is still anchored in what *McGlynn and Rackley* would describe as a corporeal and modesty based understanding of sexual violence, one which presupposes that for a crime to happen there must be the element of physical presence in terms of the act, victim and injury or harm caused.⁸

S.77, BNS or S.354 C, IPC penalises assault or criminal force with the intention to outrage a woman's modesty and S. 75 BNS addresses sexual harassment, including the electronic transmission of offensive content but requires the communication to carry a sexual overtone

⁸ McGlynn and Rackley (n 1) 537.

which is directed at the victim. That requirement may on its face be satisfied by DSSI but no court or any statute has yet authoritatively interpreted it to cover algorithmically generated content.

Section 77 BNS criminalises voyeurism, defined as capturing or disseminating images of a woman engaged in a private act. This is where the framework breaks down most clearly. Section 77 requires an act of capture which involves a physical and actual act of observation or recording. AI synthesis involves no such act instead it generates content computationally from data inputs. The statutory language of *capture, publish or transmit* cannot, without impermissible judicial expansion, be stretched to cover artificially generated content.

The Justice J.S. Verma Committee Report address this modesty standard and they recommended that sexual offence laws must shift its focus to consent and dignity instead. What they pointed out was that modesty *locates harm in societal sensibility rather than individual agency*⁹ which means that in practice, the law was protecting social reputation rather than the woman herself.

However, this suggestion was not included in the current BNS because the offence of outraging modesty exist in modified form, and they introduced no consent based framework for non physical sexual harms. So what we are left with is the same gap the Verma Committee identified in 2013, still unaddressed today.

This becomes more important when one considers that the Supreme Court by then had already weighed in on exactly this point. In the case of *Joseph Shine v. Union of India* the Court moved away from modesty based frameworks and they held that women must be treated as equal citizens with full decisional autonomy rather than passive bearers of social honour.¹⁰ So one can say that the BNS did not fully reflect the constitutional direction the Court had already indicated in their landmark judgement.

The BNS currently has no provision that specifically penalises the creation, distribution, or possession of AI-generated or synthetic sexual imagery. And this is not merely a technical omission, what it means in practice is that victims of DSSI are left without a specific criminal

⁹ Justice Verma Committee, *Report of the Committee on Amendments to Criminal Law* (Ministry of Home Affairs 2013).

¹⁰ *Joseph Shine v Union of India* (2018) 2 SCC 189

remedy, and they are forced to rely on provisions that were neither designed for nor capable of addressing this form of harm. So what we are left with is a legal silence where there should be a clear prohibition.

The IT Act, 2000 and where the act falls short

Section 66E of the IT Act 2000 penalises the capture, publication, or transmission of images of a person's private area without their consent, and they set the punishment at imprisonment of up to 3 years or a fine of up to 2 lakh rupees. Section 67A adds to this by imposing imprisonment of up to 5 years for a first conviction for publishing sexually explicit material electronically.

These provisions were a meaningful step forward at the time. However, as *Nappinai* pointed out, both were designed with authentic or real intimate imagery in mind – imagery that originates in a real photograph or recording.¹¹ What they did not account for is content that was never captured at all but generated computationally from data inputs.

The interpretive challenge is a significant one because the language of Section 66E uses terms like *intentionally captures* and *publishes* and is directed at the act of recording a real person in a real situation without their consent. On a natural reading, it does not extend to the generative act of AI synthesis which involves no capture of real imagery but rather the computational fabrication of entirely new material from data inputs – and that is a fundamentally different act from what the provision contemplates. Chesney and Citron describe this as the *liar's dividend* of generative AI. Which is the capacity to create convincing falsity without any underlying real event.¹² And it is precisely this feature that places DSSI beyond what S.66E can reasonably be interpreted to cover.

The interpretive position is further complicated by the holdings of Supreme Court in the case of *Shreya Singhal v. Union of India*. In that case, they struck down s.66A of the IT Act for being too vague, and they held that any restriction on online expression must have a clear and legitimate constitutional basis¹³. In practice it means that courts would find it difficult to stretch s.66E or s.67A to cover the generation of synthetic content, given that those provisions do not

¹¹ NS Nappinai, *Technology Laws Decoded* (LexisNexis India, 2017).

¹² Chesney and Citron (n 2) 1758

¹³ *Shreya Singhal v. Union of India* (2015) 5 SCC 1

on their face address it and in doing so would risk judicial overreach. The rule of strict construction in criminal statutes, which the Supreme Court has affirmed consistently, further limits any such reading.

Section 67B of the IT Act addresses the issue of child pornography, and it penalises those who are involved in publishing, browsing, or downloading content that depicts children in obscene or sexually explicit acts. The punishment prescribed for such an offence is imprisonment of up to 5 years for a first conviction. The provision was introduced through the 2008 amendments which means it was drafted well before generative AI became a practical reality.

Now, the critical question that arises is *Whether the phrase “computer-generated image laid down under s.67B is broad enough to extend to wholly synthetic material produced without any real child victim being involved?*

The provision is arguably broad enough to include AI-generated imagery but the main difficulty lies in the drafting of the statute itself because it is not entirely clear whether the term *depicts children* requires an identifiable real child or whether it also extends to fictional synthetic children. No court has authoritatively settled this point as yet and so the ambiguity remains unresolved.

The Digital Personal Data Protection Act 2023: Is consent a mere procedural formality?

The DPDP Act 2023 is India's most significant recent attempt at data regulation and it is an important step forward in many ways. However, its framework reflects a procedural understanding of consent that is not quite equipped to protect sexual agency in the way that victims of DSSI would need it to because the act defines *personal data* broadly as any data about an identifiable individual and they mandate a consent notice before any processing can take place. A photograph of an individual the raw material from which DSSI is generated clearly falls within this definition but the problem is that the act treats consent as a transactional authorisation for specific processing purposes and not as an expression of bodily or sexual autonomy.

According to Citron *‘the consent model of data protection treats human beings as preference satisfying machines rather than as moral agents with dignity interests that cannot be contracted*

away.’¹⁴ And what she is pointing to here is a structural deficiency that the DPDP Act reflects quite clearly.

The Act imposes a purpose limitation under s.6(1) which means that a data fiduciary who obtained a person’s photograph for a legitimate purpose, for example, a social media platform, cannot lawfully use that photograph to generate DSSI. That is a meaningful protection. However, the Act provides no specific cause of action for the sexual dignity violation that DSSI represents. So, this means that a victim can invoke the right to erasure under s.13, seek complaint resolution before the Data Protection Board, and potentially recover compensatory damages but none of these remedies address the irreversible dignitary harm that was already inflicted at the moment of generation.

The *Justice B.N. Srikrishna Committee Report* which laid down the intellectual foundation for India’s data protection framework, came closest to recognising this dimension when it described personal data as ‘*an extension of the self*’ and called for data protection to be grounded in human dignity¹⁵. That was a promising direction. However, the final DPDP Act moved away from this philosophical grounding toward procedural formalism, and what we are left with is a regime that is oriented toward compliance rather than dignity. The reform proposals set out in Part VI of this paper seek to address this gap directly.

The POCSO Act 2012 and the problem of digital child sexual material.

Section 2(da) of the POCSO Act 2012, which was inserted through the 2019 amendment, defines child pornography in fairly broad terms and what they included in that definition is any visual depiction, including any photograph, film, video, picture, computer generated image or picture, whether made or produced by electronic, mechanical or other means, of a child engaged in sexually explicit conduct. The phrase *computer generated image or picture* is interesting here, because on a natural reading it is potentially broad enough to cover wholly synthetic material generated by AI even where no real child was involved in production at all.

However, two interpretive difficulties remain unaddressed and unresolved.

- The 1st issue is that the phrase *of a child* given under s.2(da) of the POCSO Act, and

¹⁴ Danielle Keats Citron, ‘*Sexual Privacy*’ (2019) 128 Yale LJ 1870, 1880.

¹⁵ Justice BN Srikrishna Committee, ‘*A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians*’ (Ministry of Electronics and Information Technology 2018).

the question it poses is, whether this phrase extends only to an actual, identifiable and physically real human child or whether completely fictitious and synthetic children as well?

The framework of this statute is victim centric statute with the main intention to work in the and it should be interpreted in a manner that is in the best interest of the children to effectively protect them from sexual abuse and penalise the offender strictly, this is why it needs to be given a broad interpretation so that it can effectively fulfill its purpose, this was affirmed by the court in the case of *Nipun Saxena v. Union of India*¹⁶.

- There is another problem for its application because the rule of strict construction pulls in the other direction here.

What this rule essentially says is that penal provisions must be read narrowly, and where there is any ambiguity in the language, the benefit of that doubt must be given to the victim. So when this principle is applied to the term *a child* as is understood by the statute, the argument would be that it should be confined to real, identifiable children only, and not extended to fictional synthetic ones and so what we are left with is two legal principles pointing in completely opposite directions one saying interpret broadly to protect children, and the other saying interpret narrowly to protect the accused.

No court has yet stepped in to settle this conflict, at least not in the specific context of synthetic CSAM, and so the ambiguity remains very much alive.

The NITI Aayog National Strategy for Artificial Intelligence acknowledged the potential that the misuse of AI can cause in the context of child exploitation and to address this issue they recommended the implementing of a robust regulatory framework for the regulation of generative AI in sensitive domains.¹⁷

Now, this matters because it is not just an academic observation but it reflects the executive's own recognition that India's legislative framework has not quite kept pace with AI led child sexual abuse. And because that recognition comes from within the government's own policy apparatus, it lends considerable weight to the constitutional case for the reforms that this paper

¹⁶ *Nipun Saxena v Union of India* (2019) 2 SCC 703.

¹⁷ NITI Aayog, *National Strategy for Artificial Intelligence #AIforAll* (Discussion Paper, June 2018).

proposes in Part VI.

The Indecent Representation of Women (Prohibition) Act, 1986 and IT Rules, 2021 – an analysis into whether these laws effectively protects women?

The Indecent Representation of Women (Prohibition) Act 1986 prohibits the indecent representation of women in advertisements, publications, and writings but the actual difficulty is that its scope is tied to real imagery they simply did not anticipate AI generated synthetic content when they drafted it. This is because the Act was built around a mass media publishing framework like in newspapers, advertisements, commercial publications, etc. And what that means in practice is that it has no real reach over content that is algorithmically generated and privately circulated, with no commercial publishing framework involved at all.

The IT (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 place certain obligations on significant social media intermediaries and they require platforms such as Instagram, YouTube, etc. to remove non consensual intimate imagery within 24 hours of a complaint and to appoint a Grievance Officer for this purpose. This is in some respects, a step in the right direction but the problem is that the Rules do not create any substantive criminal offence for the creation of DSSI, and they impose no proactive detection obligations on platforms either. What this means in practice is that the entire burden of identifying and reporting such content falls on the victim and not on the platform that is hosting it.

This issue was specifically highlighted when a synthetically generated media of an Indian actress was circulated widely across various social media platforms and by the time the content was identified and reported, it had already reached millions of users.¹⁸

This incident led to urgent calls for legislative intervention by the Indian Government, which as a response issued an advisory to social media platforms but no specific criminal laws were invoked because no such law exists currently.

Scholars like *Vaishnavi Sharma* have documented just how inadequate this kind of reactive takedown regime is in the Indian context, and what he points out is that by the time a victim finds the content and reports it, the harm of that initial circulation has already been inflicted.

¹⁸ Deya Bhattacharya, 'Rashmika Mandanna Deepfake Video: What is It and Why is India Worried?' BBC News, (7 November 2023) <https://www.bbc.com/news/world-asia-india-67340144>

¹⁹So what the framework essentially does is respond to the harm after it has occurred, rather than taking any steps to prevent it from occurring in the first place.

Various scholars like *Franks and Waldman* have made a compelling argument in the context of deepfakes and they pointed out that '*the harm is not the persistence of the image but its original non consensual creation and circulation*'²⁰. This is an important distinction because what it essentially tells us is that a legal framework which only intervenes after the content has already been created and circulated is by design responding too late. And that is a fundamental problem, because the harm is inflicted at the moment of creation and no takedown notice, no matter how prompt can undo the harms caused to the victim.

An Analysis of Digital Sexual Imagery from Constitutional Perspective.

Article 21 of the Indian Constitution guarantees that no person shall be deprived of their life or personal liberty unless prescribed by law but the courts never interpreted the scope of A.21 in a narrow manner which can be understood through various landmark judgments. The scope of A.21 has been expanded well beyond physical liberty to include human dignity, privacy, bodily autonomy, and the right to health. That expansion is directly relevant to the harm that DSSI causes.

The Supreme Court's decision in the case of *Justice K.S. Puttaswamy (Retd.) v. Union of India* is the clearest example of this because it clearly held that the Right to Privacy is a Fundamental Right and what is particularly important is that they did not anchor it to any single provision. Instead they drew it out from Articles 14, 19, and 21 read together

On the question of State obligations as well the Court was equally clear and held that under A.21 the state has 2 obligations:

1. State must not itself violate privacy and
2. Must take active steps to protect it because restraint alone does not discharge that

¹⁹ Vaishnavi Sharma, '*Understanding Non-Consensual Dissemination of Intimate Images Laws in India with Focus on Intermediary Liability*' (2021) 14(4) NUJS Law Review

²⁰ Mary Anne Franks and Ari Ezra Waldman, '*Sex, Lies, and Videotape: Deep Fakes and Free Speech Delusions*' (2019) 78 Md L Rev 892.

constitutional duty.²¹

This concept originally came from the German Federal Constitutional Court in the *Volkszählungsurteil* also known as the *Census Case of 1983*, and it was later developed by scholars like Rodotà. This concept essentially gives people is the right to control information about themselves including the right to decide how they are represented in digital space.²²

Rodotà's idea of the *digital persona* is also useful here, because what it captures is the totality of data and representations through which a person is known in the digital world and the argument that follows from this is a significant as it says that just as a person's physical self cannot be violated without their consent, the same protection must extend to their digital self.²³

The connection between this framework and DSSI is not difficult to draw. When a perpetrator uses generative AI to fabricate a sexual image of a real person, then their action goes beyond mere misuse of data because they haven't taken digital persona of the victim and distorted it into something they never agreed to which is a sexual narrative, neither created nor consented to by the victim. The harm here is not incidental or peripheral as it strikes at the core of her identity in digital space.

Scholars like Allen developed this point further by arguing that privacy protection in the age of AI must extend to what she calls *Decisional privacy*, which is the freedom to make fundamental choices about one's body and its representations without external interference.²⁴ This concept is particularly significant in the present context because decisional privacy encompasses the right not to have sexual representations of oneself created at all and that is exactly the right that DSSI violates and it does so at the very moment of generation, before any legal action could be taken.

Gender, DSSI and Structural Inequality: An Analysis of Article 14.

The gendered nature of DSSI is not incidental because women and minor children constitute 99% of victims²⁵ and that figure alone engages Article 14's guarantee of equal protection and

²¹ *Justice KS Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1

²² Stefano Rodotà, 'Data Protection as a Fundamental Right' in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer 2009)

²³ Stefano Rodotà, 'Data Protection as a Fundamental Right' in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer 2009)

²⁴ Anita L Allen, 'Protecting One's Own Privacy in a Big Data Economy' (2016) 130 Harv L Rev Forum 71.

²⁵ Home Security Heroes (n 3)

Article 15(1)'s prohibition on discrimination on the ground of sex. The Supreme Court in *Navtej Singh Johar v. Union of India* addressed this issue directly and held that constitutional morality requires active protection of individual autonomy against both state and private encroachment. Importantly, they also held that a law's failure to protect a constitutionally vulnerable group may itself amount to discrimination.²⁶

This means that where the law fails to provide adequate criminal remedies for a harm that is inflicted systematically on the basis of sex, that failure can be characterised as institutionalised discrimination within the meaning of Article 15(1). This is because the absence of a legal remedy is not a neutral position and it sends a message about which harms does the State consider serious and which it does not.

The State's positive obligation to protect women from gender based violence is well established and grounded in the case of *Vishaka v. State of Rajasthan*²⁷ and is further reinforced by India's obligations under CEDAW General Recommendation No. 35²⁸. Taken together, these obligations require the State to take legislative action wherever an identified pattern of gender-based harm exists but as of now, that issue has not been addressed.

The current Criminal frameworks exist for analogous physical harms yet DSSI remains without a specific criminal provision. The implication of this is difficult to avoid as digital sexual violence is being treated as legally less serious than its physical counterpart. That is the kind of unequal treatment that Article 14 prohibits.

The Supreme Court in the case of *State of Punjab v. Gurmit Singh* held that sexual offences cause profound psychological injury and importantly, that this harm arises regardless of the physical modality through which it is inflicted.²⁹

This finding carries real constitutional weight because if psychological harm from sexual violation is constitutionally cognisable regardless of physical manifestation then there is no principled basis for treating the psychological harm of DSSI any differently. The victims of DSSI consistently describe their experience as indistinguishable from that of physical sexual

²⁶ *Navtej Singh Johar v Union of India* (2018) 10 SCC

²⁷ *Vishaka v State of Rajasthan* (1997) 6 SCC 241

²⁸ CEDAW Committee, 'General Recommendation No 35 on Gender-Based Violence against Women' (2017) UN Doc CEDAW/C/GC/35. <https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-recommendation-no-35-2017-gender-based>

²⁹ *State of Punjab v Gurmit Singh* (1996) 2 SCC 384

abuse which cannot be dismissed and demands constitutional recognition.³⁰

The court in the case of *Asha Ranjan v. State of Bihar* reinforced this further because they recognised that protecting victims of sexual exploitation requires both courts and the legislature to account for the systemic vulnerability of women and children. This obligation does not disappear in the digital space.³¹

The Doctrine of Synthetic Consent.

The central and original contribution of this paper is the articulation and legal operationalisation of the *doctrine of synthetic consent* which makes a specific claim that the unconsented use of a person's digital likeness to generate sexual content is a distinct legal wrong. This is because it cannot be adequately addressed by existing categories of privacy violation, data misuse, or sexual offence. Each of these categories addresses a particular aspect of the harm but none fully encompasses its entirety. So the gap that remains is what this doctrine seeks to fill. This gap is extremely important and understand why it is worth considering what each existing category actually does. Privacy law is concerned with the misuse of personal information, it asks whether data was collected and used appropriately.

Data protection law goes a step further and regulates how personal data is processed and stored. Sexual offence laws on the other hand are concerned with physical acts because it was built around the assumption that a real act, involving real persons has taken place.

DSSI fits into none of these frameworks effectively because it involves no physical act yet it causes harm that is deeply physical in its impact on the victim. It involves personal data but the harm it causes goes far beyond any data misuse. It also violates privacy and it does so in a way that existing privacy laws cannot properly address.

So what we are left with is a harm that sits in the spaces between existing legal categories.

For example, a victim of DSSI cannot point to a specific provision that criminalises and penalises the harm caused to her. She can attempt to invoke data protection law, privacy law, or sexual offence laws but each of those attempts will run into the structural limitations that

³⁰ On the harms experienced by victims of image based, see McGlynn and Rackley (n 1)

³¹ *Asha Ranjan v State of Bihar* (2017) 4 SCC 397

this paper has already identified.

This is precisely why a doctrine designed specifically for this harm is needed and section attempts to develop that doctrine with the precision required for legislative codification and judicial application.

The theoretical architecture of synthetic consent draws on four scholarly principles:

1. Through *Citron's* concept of *sexual privacy* which established that sexual agency that is the capacity to make and withhold consent in sexual contexts is a fundamental human right. This is because sexual agency and informational consent are not the same thing. For example, a person may consent to sharing a photograph without ever consenting to how that photograph is later used or manipulated.

Citron contends that sexual privacy violations undermine people's ability to control their own sexual narratives and so the law must protect not just informational interests but the deeper interest in moral and sexual self authorship of users³².

2. *Franks and Waldman in Sex, Lies, and Videotape: Deep Fakes and Free Speech Delusions* contended that non consensual deepfake imagery does not simply violate privacy rather it appropriates the victim's sexual identity entirely. And that distinction matters considerably because appropriation goes beyond violation. A privacy violation takes something from a person whereas appropriation takes over who that person is.

as contended by them, '*a digitally manipulated pornography turns individuals into objects of sexual entertainment against their will causing intense distress, humiliation, and reputational injury.*'³³

What they are identifying here is something more fundamental than harm in the conventional sense because here the victim is not simply wronged, their entire identity is replaced by a version of themselves that they never agreed to become. For example, a victim of DSSI does not merely lose control of her image. She loses control of her sexual narrative altogether and there is no legal remedy that can fully restore the harm caused to

³² Citron (n 13) 1875–80

³³ Franks and Waldman (n 18) 892.

her.

Franks also established that non consensual intimate imagery constitutes a form of identity theft but not in the conventional financial sense, instead in a deeper and more troubling sense. For example, when DSSI is created and circulated it does not just affect the victim in isolation. It shapes how others see her and it does so permanently and without her participation. This according to *Franks* is what makes this form of harm so particularly difficult to address through conventional legal categories.³⁴

3. The third tradition is *Rodotà's* framework of the digital persona and that framework is directly relevant to the present analysis because the doctrine of synthetic consent is at its core, a recognition that people have the right to control their own digital persona even in the most intimate domain possible, which is non consensual sexual representation.³⁵ So, *Rodotà's* framework essentially provides the constitutional foundation for why that right must be protected in law.

4. *Solove's taxonomy of privacy violations* adds a further dimension to this analysis because it demonstrates that the wrong caused by the creation of DSSI constitutes a dual violation. The first is what *Solove* calls *Appropriation* which happens when the perpetrator takes the victim's identity without their consent. The second is *Distortion*, which is a false sexual narrative that is fabricated to fundamentally misrepresent the victim.³⁶ Taken together, these two wrongs lead to a violation that is irreducible to either category alone. It encompasses both, and that is precisely what existing legal frameworks have failed to recognise.

The definition and legal elements

The doctrine of synthetic consent can be formally defined as: Synthetic consent violation occurs when a person's digital likeness, biometric data, image, or voice is used, without authorisation, to generate, synthesise, fabricate, or simulate sexual content, regardless of whether such content depicts actual events or is wholly fictional. The violation is complete at

³⁴ Mary Anne Franks, 'Revenge Porn Reform: A View from the Front Lines' (2017) 69 Florida Law Review 1251

³⁵ Stefano Rodotà, 'Data Protection as a Fundamental Right' in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer 2009)

³⁶ Daniel J Solove, 'A Taxonomy of Privacy' (2006) 154 U Pa L Rev 477; see also Daniel J Solove, 'Introduction: Privacy Self-Management and the Consent Dilemma' (2013) 126 Harv L Rev 1880.

the moment of generation and does not require proof of distribution, publication, or resulting demonstrable harm.

This definition has four critical structural features which are different from existing legal categories and they also provide the foundation for both criminal and civil liability.

1. Subject matter

The definition covers digital likeness, biometric data, image, or voice, etc. and this expanded scope is deliberate because the harm does not arise only from photographic likeness. It can arise equally from voice cloning, facial mapping, and other biometric modalities through which synthetic imagery can be generated. So the definition is drawn broadly enough to capture all of these.

2. The Act

This definition places a prohibition on actions that involve generation, synthesise, fabrication, or simulation of sexual content. These words were chosen for a specific reason because the wrong here is generative in nature, not distributive. And that is what distinguishes a synthetic consent violation from s.66E of the IT Act, which focuses on capture and distribution rather than creation.

3. The element of consent

The violation requires absence of informed and free consent. It is important to note that the term consent should be construed narrowly. For example, consent to be photographed does not constitute authorisation to generate sexual imagery. Similarly, consent to share a photograph on social media does not constitute authorisation to use it as input to a generative AI system. So consent in one context cannot be read across to another.

4. Content element

The content must be sexual in nature. What counts as 'sexual content' is determined by reference to whether an ordinary reasonable person would consider it as such. This encompasses explicit sexual acts, sexual nudity, and content that depicts the subject in

a sexually humiliating or degrading context. The context can be categorised separately as –

(i) Fictional content

The definition expressly covers wholly fictional content. This is because imagery of a child or adult need not depict any real event to cause real harm. This feature is particularly significant in the POCSO context, as it directly closes the interpretive gap identified earlier.

(ii) Completion at generation

The violation is complete upon generation, regardless of whether the content is ever distributed. This is the most legally significant feature of the definition. It operationalises *Franks* insight that the harm inheres in the act of fabrication itself. It also reflects *McGlynn and Rackley's* argument that image based sexual abuse constitutes a wrong independent of its consequences, which they call a *wrong per se* because it breaches the fundamental rights to dignity and privacy, as well as freedom of sexual expression and autonomy³⁷. So the harm does not begin when the content is shared. It begins the moment it is created.

4. Mens Rea, Strict Liability and the Distribution.

Any legislative codification of synthetic consent must address a critical design question. What fault standard should apply?

This paper argues that a bifurcated approach while addressing this. This is because creation and distribution are structurally distinct acts, and treating them the same way in law would be both imprecise and constitutionally problematic.

(i) Creation and the principle of strict liability

The act of generating synthetic sexual imagery of a real person without authorisation should attract strict liability. The reasons are:

³⁷ McGlynn, C., Rackley, E., & Houghton, R. (2017). 'Beyond 'Revenge Porn': The Continuum of Image-Based Sexual Abuse. *Feminist Legal Studies*, 25(1), 25-46. <https://doi.org/10.1007/s10691-017-9343-2>

1. The first reason is made clear by *Franks and Waldman* as they believed that the law allows a creator to escape liability simply because they did not intend harm, due to which sometimes the law ends up protecting the perpetrator at the victim's expense and that is not a defensible position.³⁸
2. The second reason is more straightforward because the harm here is completely avoidable. All that is required is free and informed consent before generation so there is no justification for allowing the harm to occur on the ground that intent cannot be proved.
3. The third reason concerns international consistency. The UK Online Safety Act 2023 takes this position. So does the EU AI Act, whose transparency obligations apply regardless of intent and India would not be without precedent here.
4. The Article 19(1)(a) free expression concern is also addressed through a statutory exception for artistic, research, and public interest purposes but the burden of establishing that exception falls on the accused. This means that if the accused person wishes to rely on this exception then the burden of proving it falls on them, not on the prosecution.

(ii) Distribution and the knowledge standard

Distribution of synthetic sexual imagery should attract liability where the accused knew or ought reasonably to have known that the content was generated without the consent of the depicted person and there is a sound constitutional basis for treating distribution differently. This is because the Supreme Court in case of *Shreya Singhal* clarified that there must exist a clear nexus between any restriction on speech and a legitimate state purpose. It also cautions against strict liability where unknowing intermediaries may be caught in the net. So a knowledge standard for distribution is both constitutionally sound and practically feasible.

(iii) Possession and intention standard

Possession of synthetic sexual imagery with intent to distribute should attract liability where

³⁸ Mary Anne Franks and Ari Ezra Waldman, 'Sex, Lies, and Videotape: Deep Fakes and Free Speech Delusions' (2019) 78 Md L Rev 892.

there is evidence of intent to further circulate the material. This is because mere possession does not establish the harm that the doctrine seeks to address. So the intent standard here is both proportionate and constitutionally defensible.

And this is how the three tiers work together. Strict liability applies to creation. A knowledge standard applies to distribution and similarly an intent standard applies to possession. This standard gets lower as the conduct moves further from the original wrong. That is what makes the framework calibrated and that calibration is what makes it constitutionally defensible.

The difference from General Privacy Violations

The doctrine of synthetic consent is different from ordinary privacy violations in three different ways.

- i. The first difference is that it is prospective rather than retrospective. An ordinary privacy violation usually discloses something that already exists and is true and the synthetic consent violation does the opposite because it creates a false sexual narrative that had no prior existence at all. So the wrong here is not that something real was exposed. It is that something entirely new was fabricated.
- ii. The second difference is that it is identity constituting, not merely informational. A general or ordinary privacy violation reveals something about the victim and a synthetic consent violation goes further than that. It creates a new fact about the victims which could be completely false without having any power to retract or correct it. For example, a conventional privacy violation might expose a private photograph and a synthetic consent violation invents a sexual identity that the victim never had and never agreed to.
- iii. The third difference is irreversibility. Once synthetic sexual imagery has been generated the victim cannot unconsent after the fact. The violation is complete the moment it is created and erasing it later changes nothing. This is because the harm is caused when the content comes into existence and not when someone sees it.

These three differences set synthetic consent apart from anything the existing law was built for. So what we are left with is a wrong that is sui generis which the current Indian data protection law cannot fully address it neither the privacy law and not the sexual offence laws. That is

exactly why it needs specific legislative recognition of its own.

Lessons for reform: A comparative analysis with various legal frameworks.

i) The United Kingdom:

The United Kingdom offers the most instructive comparative model for Indian reform and that is because its law did not remain static. It began by regulating distribution and progressively moved towards regulating creation and that is exactly the trajectory Indian law now needs to follow.

The starting point was S.33 of the Criminal Justice and Courts Act 2015. Under that section sharing an intimate image without consent of the victim was an offence only where the prosecution could prove that the defendant had intentions to cause distress to the victim.³⁹

This appears reasonable in principle but in practice it set the threshold far too high because the perpetrator needed only to prove some alternate intent like it was a joke or that it was done for financial gain or that it was shared without proper thought and the case would usually collapse and because to this the people the law was aimed to protect were the ones it failed most consistently.

But this logic was abandoned when Online Safety Act, 2023 was enacted because this act instead of asking why the material was shared, it asked ***Whether it should have been created or shared at all in the first place?***

This shift is more significant than it first appears because it relocates the wrong and the injury is no longer treated as something that occurs when an audience views the image instead it is treated as something that occurs earlier at the time of the creation of the image. And once that is accepted the question of intent becomes irrelevant.

This is also why the UK model addresses the problem of irreversibility. By the time content has been created no measure of takedown or deletion can undo the harm that already been caused to the victim. A law which is built around distribution of the sexual imagery simply cannot address this harm effectively because it operates only once the material has been circulated or

³⁹ Law Commission, 'Intimate Image Abuse: A Final Report' (Law Com No 407, 2022) Justice UK <https://share.google/R3uHvpbjZAr2jxAbj>)

published. The UK's response was to intervene before that stage which is precisely the form of intervention India still lacks.

The lessso is not that the United Kingdom resolved every difficulty but that their efforts are grounded in protecting the dignity of the victims and penalising the offenders. India should not replicate where British law began because that starting point reflects the same flaws our own framework now exhibits.

The Online Safety Act 2023 added sections 66A and 66B into the Sexual Offences Act 2003, which criminalises the sharing of or giving threats to share a person's intimate images which includes synthetically generated sexual content such as deepfakes without the informed consent of the victim.⁴⁰ This moved away from the traditional requirement of intention under which the prosecution had to prove that the accused acted with the purpose of causing distress to the victim. Now in the UK, it is enough that the image was shared without the consent of the person depicted regardless of why the accused chose to share it.

This shift drew on the *Law Commission's Final Report on Intimate Image* gave the ground work for the reforms. In it, the Commission held that the harm to a person's dignity in cases of non consensual sexual imagery comes from the creation and distribution itself and does not depend on the intentions of the accused.⁴¹ This is very much in line with the doctrine of synthetic consent that this paper puts forward.

The Data (Use and Access) Act 2025 went a step further as Section 138 added new sections 66E to 66H to the Sexual Offences Act 2003 as a result of which from 6 February 2026, creating a purported intimate image of a person without their consent became a criminal offence in its own right.⁴² This section goes even wider because it also penalises a person who simply asks for such an image to be made, whether or not the image is ever actually produced.

This is not a strict liability offence even though it is sometimes treated as one. In practice the prosecution still has to prove two things. The first thing is that the accused created the image intentionally and secondly it has to be proved that they had no reasonable belief that the person

⁴⁰ Online Safety Act, 2023

⁴¹ Law Commission, 'Intimate Image Abuse: A Final Report' (Law Com No 407, 2022) Justice UK <https://share.google/R3uHvpbjZAr2jxAbj>

⁴² The Data (Use and Access) Act, 2025

had consented to it.

But what really matters is where the law locates the wrong. The offence is treated as complete the moment the image is created and not when it is shared or seen by someone else. This is the very conclusion that this paper has been arguing towards. India would do well to draw on this approach but it has to do so with caution because the model cannot simply be copied, instead it needs to be adapted to fit the Indian constitutional framework.

ii) South Korea

South Korea's legislative response to the *Nth Room* which was a Telegram based deepfake sexual abuse network is an extremely important case study to understand how a state should respond to documented mass victimisation. The Act on Special Cases Concerning the Punishment of Sexual Crimes was amended in 2020 to insert Article 14-2 which criminalised the editing or processing of images to cause sexual desire or shame without the consent of the person who has been depicted.⁴³

The penalty for creation and distribution was initially set at a maximum of 5 years imprisonment but what is important here is that the Korean legislature revisited and strengthened this framework in September 2024 because it recognised that the original provision was unable to adequately address the issue.

The September 2024 amendment raised the maximum sentence for creating and distributing deepfake sexual material to 7 years imprisonment but more importantly, it also criminalised the possession and viewing of such material which is now punishable by up to 3 years imprisonment or a fine of 30 million won.⁴⁴

This development is directly relevant to the Indian reform proposals because it shows that even a well designed initial response may require iterative strengthening as the true scale of the problem becomes clearer and it also introduces a possession offence which is exactly what this paper proposes for India as well.

⁴³ Act on Special Cases Concerning the Punishment of Sexual Crimes (South Korea), art 14-2 (inserted 2020; maximum sentence raised to seven years and possession and viewing criminalised by amendment of September 2024).

⁴⁴ Act on Special Cases Concerning the Punishment of Sexual Crimes (n 37)

The Korean model also shows that the connection between legislative reform and comparative law methodology. The 2024 amendments were made by an analysis of the UK and EU regulatory developments which illustrates the value of a purposive comparative engagement and this is precisely the methodology that this paper employs. The lesson for Indian reform is not to blindly import the Korean provision but to apply its underlying principle which is a creation focused framework with strict liability for generation, stricter and harsher punishments for organised or commercial distribution, and a separate possession offence.

iii) The European Union

The European Union's regulatory framework operates across 2 complementary instruments which together address both platform accountability and AI system governance and this is a dual architecture that the Indian reform should replicate. The Digital Services Act 2023 imposes obligations on large user base online platforms like Instagram or WhatsApp to conduct systemic risk assessments concerning technology facilitated gender based violence which includes deepfake pornography under Article 34(1)(d), risk mitigation measures under Article 35, and penalties in the fines of up to 6% of their global annual turnover for non compliance under Article 74(2).⁴⁵

The EU AI Act 2024 addresses the AI system creators and distributors. It is important to clarify here that deepfake sexual imagery generators are not classified as unacceptable risk AI systems under Article 5 because this is a category which is reserved for things like social scoring, biometric scraping and real time law enforcement biometric identification.

Instead, the AI Act addresses synthetic sexual content through mandatory transparency obligations which means that creators of AI systems that generate or manipulate image, audio, or video content depicting real persons must ensure that the outputs are machine readable and marked as artificially generated under Article 50(2) and must ensure a prominent disclosure where the content constitutes a deepfake irrespective of the purpose and intention under Article 50(4).⁴⁶

⁴⁵ Digital Services Act, Regulation (EU) 2022/2065 of the European Parliament and of the Council [2022] OJ L277/1, arts 34(1)(d), 35 and 74(2).

⁴⁶ Artificial Intelligence Act, Regulation (EU) 2024/1689 of the European Parliament and of the Council [2024] OJ L1689, arts 5, 50(2) and 50(4); European Commission, 'Guidelines on Prohibited Artificial Intelligence Practices' (4 February 2025).

The direct relevance of the EU framework to the Indian reform lies in its institutional architecture rather than in its specific prohibitions. The DSA's systemic risk assessment model which requires platforms to proactively identify and mitigate DSSI risks rather than merely reacting to complaints is the appropriate model for the amendment of India's IT Rules 2021.

The AI Act's transparency obligations also provide a template for the algorithmic accountability framework proposed in Part VI. Scholars like *Griffin* believe that the DSA's Article 34 systemic risk framework if it is properly implemented, can extend to gender based violence in ways that complement rather than duplicate criminal prohibitions and this is a lesson that is directly applicable to the design of India's intermediary obligations.⁴⁷

What the Indian legal system should draw from the comparative analysis

- I. The comparative analysis above supports four specific conclusions for the Indian legal reform. First is that India should adopt a creation focused criminal offence which is consistent with the UK's post 2026 framework rather than limiting itself to the distribution focused approach of the pre 2026 law.
- II. Secondly, India should adopt a stricter penalty system which is consistent with the Korean model which means strict liability and substantial imprisonment for creation, knowledge based liability for distribution, and an intent based possession offence.
- III. Third, India should adopt a dual regulatory architecture which is consistent with the EU model which is a criminal or civil liability framework for creation and distribution that is supplemented by a systemic risk assessment and mitigation framework for the platforms.
- IV. Fourth, all the 3 comparative models reach to the same conclusion that the appropriate normative foundation is the victim's dignity and sexual autonomy and not the obscenity or public morals framework that currently characterises the Indian law and this is a conclusion that is consistent with the doctrine of synthetic consent and with the Supreme Court's own trajectory in the cases of *Joseph Shine*⁴⁸ and *Navtej Johar*⁴⁹.

⁴⁷ Rachel Griffin, 'Governing Platforms through Corporate Risk Management: The Politics of Systemic Risk in the Digital Services Act' (2025) 4 European Law Open 223

⁴⁸ *Joseph Shine v Union of India* (2019) 3 SCC 39

⁴⁹ *Navtej Johar v Union of India* (2018) 10 SCC 1

The proposed legal reforms.

i) Adding a Deepfake and Synthetic Sexual Media Clause under the existing criminal laws.

This paper proposes that a dedicated deepfake and synthetic sexual media clause must be added within the Bharatiya Nyaya Sanhita 2023. The proposed provision should operationalise the doctrine of synthetic consent with strict liability which would reflect the inherent harm of generation. It should also adopt a knowledge standard for distribution and must be consistent with the holdings of the court in the case of *Shreya Singhal v. UOI*⁵⁰. It should also introduce an offence for the possession of DSSI which would be consistent with the Korean model.

ii) Codification of Synthetic Consent in the existing civil law.

The doctrine of synthetic consent should also be codified as a standalone civil cause of action, available independently of any criminal prosecution. A victim should be given the right to bring a civil claim for synthetic consent violation without the proof of criminal intent or any monetary harm.

- The available remedies should include: A mandatory injunction mandating the erasure of all copies of the synthetic imagery and deletion of all data used in its generation.
- The compensation of damages of not less than Rs 5 lakhs per incident, without proof of actual loss, reflecting the inherent dignitary harm.
- There must be exemplary damages given where the violation was commercial or organised.

The Data Protection Board which was established under the DPDP Act 2023 should also be empowered to adjudicate civil synthetic consent claims in addition to its data protection functions, with an broader jurisdiction to award exemplary damages for dignitary harm. The DPDP Act should also include a specific category of sexual persona data, which means the biometric and photographic data whose misuse in the sexual domain constitutes a

⁵⁰ *Shreya Singhal v Union of India* (2015) 5 SCC 1

categorical violation of sexual agency which requires the strictest level of data protection obligations and remedies.

iii) The algorithmic accountability framework for Generative AI

Following the EU AI Act's transparency model, India should establish an algorithmic accountability framework for generative AI platforms. This framework should include:

- A mandatory registration of all generative AI systems capable of producing human likeness imagery with the proposed Data Protection Board or a dedicated AI regulatory authority.
- There must be technical safeguard implemented including the implementation of consent verification systems before generating imagery of identifiable real persons.
- There must be a mandatory impact assessments before deployment of generative AI systems capable of producing sexual content.

A failure to implement required safeguards effectively should give rise to strict civil liability for any synthetic consent violation created by the software, irrespective of whether the software had actual knowledge of the specific violation. This reflects the principle that was recognised in the EU's DSA framework, that platforms which deploy technology capable of causing systemic harm bear a proportionate systemic responsibility for that harm.

CONCLUSION

The algorithmic sexualisation of women and children through AI generated deepfake sexual imagery represents one of the most pressing human rights challenges of the modern digital age. And India's existing legal framework is constitutionally and doctrinally inadequate to address this issue because of the BNS's modesty based laws, the IT Act's distribution focused provisions, the DPDP Act's procedural consent formality, and POCSO's interpretive challenges collectively fail to provide victims with adequate criminal or civil remedies.

- This paper has tried to provide a comprehensive doctrinal analysis of India's statutory gaps and moved beyond descriptive observation to identify the interpretive limits of each provision and the possible constitutional violations.

- It also developed the doctrine of synthetic consent with defined elements like mens rea, and also pointed at how is this different from the existing legal categories.
- In this paper, a purposive comparative analysis linking international developments directly to Indian reform proposals was also given rather than simply describing foreign law.
- It has also proposed a concrete, constitutionally grounded legislative reforms, like, introducing DSSI as a specific BNS offence, a civil cause of action and an algorithmic accountability framework.
- These reforms are demanded by India's constitutional commitment and are reflected in progressive interpretation of the court in cases of Puttaswamy, Joseph Shine, Navtej Johar, and Asha Ranjan and also by its international obligations under CEDAW, the CRC, and the Budapest Convention. The Justice Verma Committee's opinion that Indian law must move beyond modesty toward consent and dignity has not been fulfilled in the digital domain. The doctrine of synthetic consent is the next chapter in that unfinished jurisprudential journey.

As the Supreme Court held in *Maneka Gandhi v. Union of India*, the Constitution is a living instrument to be interpreted in light of the evolving needs of society⁵¹. In the algorithmic age, the importance of digital dignity, sexual privacy, and informational self determination demand nothing less than comprehensive and urgent legislative reform.

The architecture proposed in this paper has tried to provide a constitutionally grounded, comparatively informed, and doctrinally coherent foundation for that reform.

⁵¹ *Maneka Gandhi v. Union of India* (1978) 1 SCC 248