International Journal of Multidisciplinary Science and Innovation (IJMSI)
Website: https://ijmsi.in/
ISSN: 3107-5754
Vol. 2, Issue 1, Jan-Jun, 2026
Page No.: 23-32

Review

Digital Intimacy and the Law: A Study on Consent, Privacy, and Punishment under the Bharatiya Nyaya Sanhita

Preeti
LLM Student, Amity University, Gurugram

Corresponding Author:
Imroj Khan

Email:
choudharypreeti1999@gmail.com

DOI: *10.62896/ijmsi.2.1.04*

Conflict of interest: *NIL*

Article History
Received: 05/12/2025
Accepted: 20/01/2026
Published: 28/01/2026

Abstract:
The Bharatiya Nyaya Sanhita (BNS), 2023, is a significant legal development in India's approach to digital-mediated intimacy-related offenses. Nonetheless, the fluid nature of the digital consent, as well as the development of new/novel technologies, including deepfakes and AI-generated content, makes the BNS less effective in its fight against digital sexual harms. This paper is a synthesis of the recent research works as it aims to explore the response of the BNS to its changing conceptualisation of consent, privacy and accountability in the digital intimacy. It highlights the weaknesses of the BNS gender-specific problems, lacking implementation procedures, and gaps in the evidence that fail to capture the relationship and contextual nature of digital violations of consent. The paper suggests legal changes, which include a dedicated offence of digital intimacy harms, which is not gender-based, the positive elements of consent, and the responsibility of platforms. It further reiterates the necessity of specialised training in cyber forensics, victim-oriented enforcement practices, and judicial training on a relational-based consent model. These reforms are expected to develop a culturally sensitive legal ecosystem that supports individual autonomy, privacy and dignity online and to respond to the gendered power imbalance and technological incomprehensiveness of digital sexual violence.

Keywords: Digital intimacy, Consent, Privacy, Accountability, Bharatiya Nyaya Sanhita, Feminist legal theory, Digital consent theory, Expressive punishment theory, Non-consensual dissemination of intimate images, Voyeurism, Cyberstalking, Sextortion, Deepfakes, Victim-blaming, Social stigma, Platform governance.

INTRODUCTION

The digital intimacy of the era of ubiquitous connectivity has challenged the conventional concept of consent, privacy and accountability, requiring a redefinition of the law. The Bharatiya Nyaya Sanhita provides a critical view, in relation to which these changing dilemmas, in particular, can be viewed as digital interactions, where the line between personal autonomy and harm is becoming increasingly unclear. This study investigates how the law responds to these shifts and whether its punitive structures adequately address the realities of technologically mediated intimacy.

The research title had been situated within a multi-theoretical framework that drew on feminist legal theory, privacy as dignity theory, digital consent theory, and expressive punishment theory to analyse digital intimacy under the Bharatiya Nyaya Sanhita (BNS). Feminist legal theory had framed digital sexual harms such as voyeurism, non-consensual dissemination of intimate images, and technology-facilitated sexual violence as extensions of gender-based violence embedded in power asymmetries, thereby informing a critical reading of BNS provisions on offences against women and children and their enhanced penal responses.Privacy as dignity theory, grounded in Indian constitutional jurisprudence on informational and decisional privacy, had been used to conceptualise digital intimacy as an aspect of

personhood, so that offences like voyeurism and revenge porn under the BNS–IT Act matrix were treated as violations of autonomy and dignity rather than mere obscenity or morality concerns. Digital consent theory, developed in scholarship on platform governance and image-based abuse, had reconceptualised consent as an ongoing, contextual, and revocable process in online environments, which guided the assessment of how BNS provisions interfaced with IT Act sections on capturing, transmitting, and publishing intimate content without consent, and whether the statutory language adequately reflected granular forms of coercion, manipulation, and power imbalance in digital interactions. Expressive and consequentialist theories of punishment had underpinned evaluation of the BNS's calibrated sentencing structure—including stringent minimums and aggravated forms for sexual and privacy-invasive offences—to examine whether increased penalties and the symbolic consolidation of crimes against women and children in a dedicated chapter normatively communicated societal condemnation and effectively advanced deterrence, retribution, and victim-centric protection in the context of digital intimacy.

The research on "Digital Intimacy and the Law" had engaged with three interlinked dynamics: emerging trends in technology-mediated intimacy, persistent doctrinal and structural issues, and evolving enforcement and governance challenges. Recent trends had included the rapid proliferation of non-consensual dissemination of intimate images (NCII), deepfakes, sextortion, cyberstalking, and voyeuristic recording and sharing of intimate acts, often facilitated by ubiquitous smartphones, social media platforms, and AI-driven content manipulation tools. At the same time, statutory reform through the Bharatiya Nyaya Sanhita, read with the IT Act and the Digital Personal Data Protection Act, had signalled a shift towards stronger penal and consent-based frameworks for digital privacy and sexual autonomy, particularly via specific offences on voyeurism, stalking, and privacy violations. However, the research had identified key issues such as fragmentation and overlap between BNS, IT Act, and data-protection norms, the absence of a dedicated NCII offence, gendered and relationship-contingent drafting, and courts' continued reliance on obscenity or modesty paradigms rather than privacy, autonomy, and dignity as the central organising principles.Challenges had further arisen at the levels of proof and consent—especially in relation to screenshots, metadata, deepfakes, and implied or relational consent—alongside under-reporting driven by victim-blaming, social stigma, and fear of further circulation of content, which collectively undermined the victim-centric objectives of BNS reforms. Finally, the study underscored systemic enforcement and governance challenges, including slow takedowns and inconsistent platform cooperation despite emerging NCII takedown protocols, limited cyber-forensics capacity, and inadequate gender-sensitive training of police and judiciary, which had constrained the practical effectiveness of enhanced punishment provisions and highlighted the need for integrated legislative, platform-regulatory, and institutional reform.

The issue that the study aimed to address was that, due to the rapid growth of technology-mediated relationships and the circulation of intimate digital content, the conceptual and doctrinal understanding of consent, privacy, and punishment in the Bharatiya Nyaya Sanhita was significantly lacking and inconsistent. Even though the BNS created and centralised offences like voyeurism, cyberstalking and other technology-mediated sexual harms, the statutory expression and enforcement culture still grappled with subtle issues over digital consent (including revocability, coercion and situationality), informational and decisional privacy protection in intimate contexts and proportionality and effectiveness of the criminal response to a digital environment where harms are immediate, non-localised and easy to copy.It's a major issue in a country like India because of its victim-blaming blaming deep-rooted patriarchal society, which leads to gender inequality which making it difficult to get justice. Simultaneously, the disjointed relations between the BNS and information technology regulation and data protection norms did not allow the harmonious protection of the digital sexual autonomy of individuals. The study was thus justified and relevant since it conducted a systematic review of whether and how the BNS was responding adequately to the digital intimacy reality, whether and how there were doctrinal and practical gaps in dealing with harms like non-consent dissemination of intimate images and deepfakes, and attempted to inform legislative, judicial, and policy changes to make criminal law more victim-focused, privacy-

conscious, and technologically sensitive in the era of ubiquitous digital intimacy.

OBJECTIVES

- To discuss the effects of digital intimacy practices on the conceptualisations of consent and privacy within the Bharatiya Nyaya Sanhita.
- To test the role of privacy weaknesses, power, and enforcement mechanism in legal and punitive redress to the harms of digital intimacy.
- To find out and determine the qualitative measures of consent clarity, privacy risk, and enforcement effectiveness in cases of digital intimacy.

Since the conceptual background and the main objectives of the current work were outlined, it is necessary to place the investigation into the context of the existing scholarly and legal discussions. The literature review presented below is a synthesis of the existing research on the topics of digital intimacy, consent, privacy, and punitive frameworks with an emphasis on the existing gaps that justify the necessity of an exploratory, qualitative investigation within the framework of the Bharatiya Nyaya Sanhita. This review therefore gives the analytical foundation on which the further analysis is built on.

LITERATURE REVIEW

Perceive consent:

The parameters of consent have been transformed by digitally mediated intimacy, which has been enabled by dating applications, social media, and online communication platforms. The conventional legal approach to the concept of consent that is frequently based on physical interactions, cannot meet the challenges posed by virtual interactions. The scholarship after 2023 discusses how users understand online sexual interactions and consent, and how legal practitioners are reacting to this new set of rules.

Yujia Zhu's Dating Apps and Social Media: The Blurring of Boundaries in Sexual Assault and Consent argues that digital mediation creates psychological and legal ambiguity surrounding consent, particularly in non-physical sexual coercion and "contextual withdrawal" of consent.Zhu states that the concept of consent in the context of digital mediation is perceived by the user as dynamic and reversible, as opposed to the legal system, which perceives consent as static and as existing at the moment of.

Similarly, Patrocino and Bevilacqua in The Autonomy and submission in digital self-exposure and Violent Exposure of women examine how digital representations (e.g., nudes, sexting) blur the boundary between bodily and virtual autonomy. They find that participants view the sharing of images as a form of conditional consent, limited by context and trust, whereas legal frameworks continue to treat such dissemination as binary—either given or not.

The issue of the moment of consent in digital contexts is an area that is being increasingly recognized by legal practitioners as being more than just a one event phenomenon. The report of SCCJR by Michele Burman, Olivia Smith, Oona Brooks-Hay and Yassin Brunger has stated that lawyers perceive sexual online communication using evidentiary paradigms that are inappropriate in emotional contexts. According to them, courts are being text-based, meaning that they favor chat logs and timestamps, rather than intent, tone, or relational context.

Furthermore, Neil Richards and Woodrow Hartzog critique how evidentiary practices fail to capture digital coercion, where algorithmic suggestion or platform pressure influences consent. Her study with Scandinavian prosecutors reveals growing frustration with proving non-consensual digital intimacy in law, despite victims' clear subjective distress.

Amelia E. Evans in Negotiating Digital Sexual Consent When Sending a Nude Image discovered that people negotiated consent as an ongoing process, especially when in lengthy online relationships. In their qualitative interviews, the users state that trust, reciprocity, and revocability are the major indicators of digital consent validity. Notably, respondents considered the screenshotting or passing on messages as a form of consent since they did not necessarily have to be in physical contact

Similarly, Doug and Nick (2023) point at gender disparities in the interpretation of digital consent. Women commonly complain of emotional coercion in situations of persistent requests and men in mixed signals because of the asynchronous communication. This movement highlights the time-based complexity of consent on the Internet

In the jurisprudential perspective, Wu and Zhang(2023), suggest that digital consent ought to

be viewed as a communicative process that occurs repeatedly but not as an event. This is consistent with the feminist legal theory, which puts more emphasis on the continuing negotiation rather than a formalistic definition. In the meantime, Sylwander(2025) suggests a set of statutory measures, using affirmative digital consent, indicating that app-based logs might be presented as legal evidence in case it is available.

Nevertheless, critics like Moniz, Mehrnezhad, and Almeida raise the risk of privacy violations when films on intimate consent are digitized, and that datafication of desire can be counterproductive in eliminating autonomy.

Reshape privacy norms

Digital intimacy practices, such as sharing private images, sexting, and AI-generated deepfakes, expose vulnerabilities in India's criminal laws by blurring consent boundaries and amplifying non-consensual dissemination risks. These practices challenge traditional privacy notions under the Bharatiya Nyaya Sanhita (BNS), 2023—which replaced the Indian Penal Code (IPC), 1860—and highlight gaps in addressing technology-driven harms.

- Legal Framework Overview

BNS Section 77 mirrors IPC Section 354C on voyeurism, criminalising non-consensual capture or sharing of women's private act images, with 1-3 years' imprisonment for first offenses and 3-7 years for repeats, yet remains gender-specific and excludes digitally altered content like deepfakes. Provisions under the Information Technology Act, 2000 (Sections 66E, 67A) punish privacy violations and explicit content transmission but react reactively, lacking proactive tools like mandatory platform hash-matching. The Digital Personal Data Protection Act, 2023, enables data erasure but faces enforcement delays via the nascent Data Protection Board.

- Challenges from Digital Intimacy

Non-consensual intimate image sharing (NCII), including deepfakes and sextortion, fragments privacy protections as BNS/IPC focus on punishment over prevention or victim support, ignoring synthetic media's scale. Patriarchal enforcement biases deter reporting, with police often victim-blaming or lacking digital forensics, exacerbating psychological and reputational harms disproportionately on women. BNS modernizes cybercrime recognition—treating some as organized offences with harsher penalties—but omits clear definitions for emerging threats, risking overlaps with IT Act provisions.

- Reshaping Privacy Notions

Digital practices compel redefining privacy from physical to informational autonomy, as affirmed in *K.S. Puttaswamy v. Union of India*, yet BNS/IPC's narrow scopes fail evolving harms like AI manipulation. Judicial trends, such as *Mrs X v. Union of India* mandating takedowns and FIRs, innovate remedies but strain under jurisdictional limits and platform non-compliance. Reforms urged include gender-neutral standalone offences, platform accountability, and training to align laws with digital consent dynamics.

Digital Intimacy and Privacy Risks Conceptualisation.

Digital intimacy is a concept that involves various acts, including the sharing of personal information to the extent of having emotionally meaningful interactions through the digital medium. Although they help to connect, these interactions pose significant privacy threats. The commercial threat model of digital intimacy identifies vulnerabilities like unauthorised access to data, non-consented sharing, and stigmatisation of some groups (in particular, sex workers), which increase the effects of privacy violations. The absence of strong technical protection and continued existence of stigmatisation also aggravate these threats, necessitating a research agenda focused on safer digital intimacy practice.

- Manifestations of Privacy Breaches

There are multiple ways privacy is violated in digital intimacies:

Datafication and Commodification: Dating applications and social networks transform intimate actions into data, which is subsequently commodified and can be used by applications to generate business. Such a process subject the users to the risk of surveillance, misuse of data, as well as loss of control of personal information.

Non-Consensual Distribution: Revenge porn and image-based sexual abuse are horrifying privacy invasions that turn the means of trust into the methods of coercion and control. A lot of these violations are gendered, and women become the most frequent victims of such behavior, and anonymity and accessibility on digital platforms facilitate these violations.

Cyber-Dating Abuse: Technologies enable the emergence of new types of intimate partner violence, such as monitoring, control, and surveillance, and young women are more severely affected. These power imbalances are usually supported by societal norms and the design of platforms.

Digital Intimacy Asymmetries of Power.

Power imbalances are fundamentally ingrained in the online intimate relationships:

Algorithmic and Platform Power: Platforms command a lot of power because of obfuscated algorithms and data policies, usually without the notice or any meaningful consent by the user. This situation gives rise to a sense of resignation and cynicism among the users, who find themselves helpless in relation to institutional data practices.

Gendered Dynamics: Digital intimacy is informed by established provisions of male domination, where girls and activities of women are more subject to scrutiny and policing. These imbalances can be seen in the architecture of digital space and in the social conventions that determine its usage.

Boundary Negotiation and Trust: Privacy boundaries in intimate relationships tend to be negotiated implicitly, and there is the concept of privacy silence that comes out as a tactic not to confront. However, such violations as unauthorized access to devices can diminish trust and strengthen power asymmetries, particularly those of coercive control.

- Psychological and Social Impacts

The psychological distress of privacy invasion in digital intimacy is associated with anxiety and depression. The privacy paradox in which users are concerned, but they still have risky behaviors demonstrates the difficulty of privacy management in the digital world. Platform and partner manipulations also make the choice and well-being. of users less significant.

Enforcement

The Bharatiya Nyaya Sanhita, 2023 (BNS) is an important change of direction in Indian criminal law, especially regarding digital harms, such as those that come with digital intimacy. This review will focus on how the punitive provisions of the BNS have been interpreted and applied by the enforcement agencies in such cases based on new scholarship published after 2023.

- Interpretation and Application by Enforcement Agencies

The BNS features new definitions and processes of dealing with cybercrimes, such as those that could be perpetrated; digital intimacy, such as non-consensus sharing of intimate photos, cyberstalking, and online harassment. The application of these new provisions by enforcement agencies involves adapting to them and as such, they focus on the collection and admissibility of digital evidence. Singh and Pandey observe that the BNS, the Bharatiya Nagarik Suraksha Sanhita (BNSS) and the Bharatiya Sakshya Adhiniyam (BSA) simplify the process of collecting and prosecuting digital evidence, in a bid to ensure that enforcing it becomes more effective in the digital era. Nevertheless, they also raise some issues which remain, including the lack of privacy, destruction of evidence, and gaps in the forensic infrastructure, which can impede the practical implementation of punitive provisions in the case of digital intimacy harms.

- Challenges in Enforcement

Although the BNS has a progressive purpose, the enforcement agencies experience a number of challenges:

Forensic and Investigative Capacity: Digital evidence is needed, and better infrastructure to manage cyber forensic training is required to deal with digital intimacy cases.Jurisdictional and Privacy Issues: Digital evidence presents complexities to digital crime investigation and prosecutions due to the cross-border nature of digital crimes and privacy issues

Interpretative Ambiguity: Researchers claim that although the BNS modernizes the law, there is still some uncertainty when it comes to interpreting new crimes, particularly those committed by women and children in cyberspaces.

- Gendered and Victim-Centric Approaches

According to the recent examination, the BNS tries to resolve the issue of offences against women and children more extensively, yet the efficiency of the provisions depends on the interpretation and prioritization of the victim-focused strategies by the enforcement agencies. Singh cites the significance of sensitivity and special procedures in addressing the damage of digital intimacy because of the psychological and social effects that are peculiar to victims.

- Comparative and Critical Perspectives

Comparative analysis of the BNS and the Indian Penal Code (IPC) also brings to the fore

improvements made as well as the areas of resilience. Although the BNS is perceived as a positive move towards acknowledging the digital harms, Dixit expresses his worries as to whether the new code is progressive enough or the code sustains retrogressive silences more so in sexual offences and digital intimacy. A critical analysis by Naik also highlights the significance of specifications and judicial review so as to make sure that punitive provisions are implemented in a fair and efficient manner .

- Effectiveness of Legal and Enforcement Processes

The Bharatiya Nyaya Sanhita, 2023 (BNS) is an important legislative change in the Indian attitude towards intimate-related crimes digitally mediated. The presented review summarizes the recent research (post 2023) to assess the efficacy of BNS-based legal and enforcement procedures with xenophobia-centered qualitative variables analyzed, including protection of the victims, evidence standards, gender sensitivity, and responsiveness of the institution.

- Legal Reforms and Evidentiary Challenges

The BNS also adds the new provisions to cover digital sexual exploitation, such as such crimes caused by false promises of marriage and non-consent digital behaviors. This analysis by Bajpai shows that although the BNS criminalizes new, not previously criminalized, types of sexual exploitation, its efficacy relies on the interpretative clarity and enforcement that is gender-sensitive. The paper observes that there are always insurmountable obstacles in evidence, the chances of abuse, and a society-wide prejudice that hinder the uniform utilization and safety of the victims. The necessity to have well-defined judicial practices and train the police is underlined to avoid biased justice and be able to create deterrent effect of the law.

Singh and Pandey discuss the wider cybercrime environment within BNS and associated laws and report positive changes in the digital evidence-gathering and prosecution. They however note that despite all these, there are still challenges facing it like issues of privacy, alteration of evidence, jurisdictional challenges and a lack of forensic infrastructures. The authors recommend special cyber forensic training and better investigative ability to increase efficiency of enforcing cases of digital intimacy cases

- Gender Inclusivity and Victim-Centric Approaches

The current literature is quite critical of the BNS method of being gender-neutral and protecting vulnerable populations. According to Bajpai and Gupta, the BNS has been wanting to address past legal vices, but it is not sufficient in offering gender-neutral safeguards especially on the side of men and transgender individuals. This is a shortcoming that impacts on the inclusiveness and perceived fairness of the enforcement of digital sexual offences. Shrivastava and Akhter also believe in the necessity to acknowledge rights of LGBTQIA + and historical gender inequalities in the new legal system.

Institutional Responsiveness and Societal Impact

The review of sexual offences by Dixit's nder BNS raises questions as to whether the reforms are real advancement or recidivism of the regressive silences particularly in the context of digital harms. The issue that the study addresses is the need to enforce in a more proactive and victim-centred manner and greater institutional responsibility through which the legal changes may be transformed into the actual protection and redress. This analysis by Rizvi's of gender-based violence on online space highlights the necessity of multi-layered solutions such as enhanced legal safeguards, responsibility on the part of the platform, and social awareness to the transnational and long-standing nature of online gender-based violence.

- Comparative and Critical Perspectives

Comparative analyses of the BNS and the Indian Penal Code (IPC) point to some improvements and some areas of consistency. According to Gopal, in the comparative analysis, it is implied that despite the BNS modernizing the legal landscape, its effective application in the case of digital intimacy will depend on the continuity of interpreting the law, enforcing the law, and adjusting to the emerging types of digital threats.

RESEARCH METHODOLOGY

This article uses a qualitative research methodology; it is a theoretical research study in which secondary information from various writers and researchers was used to gather the necessary data. Books, journals, newspapers, and various reports on the subject as well as related publications, were examined by the researcher, whose name is mentioned.

DISCUSSIONS

Digitally mediated intimacy is transforming perceptions and regulation of consent, privacy, and

accountability in the law. The reviewed scholarship shows a crucial change in the traditional and event-based conceptualization of consent to a dynamic, relational, and technologically situated conceptualization. The emergence of dating applications, social media connection, and AI-mediated communication has blurred the distinct lines that existed between what was public and what was private, or consent and coercion. Consent in the realm of digital interaction, as Yujia Zhu and later thinkers suggest, cannot be well-received with the help of the statical perspective, i.e. as a one-time permission or refusal to permit something, but as a process of negotiation that can and probably should be continued, and that is shaped by context, trust, and revocability.

It can be elaborated by research published by Evans and Doug & Nick, which sheds light on gendered experiences and the temporal discontinuities that make online consent even more problematic. Females commonly complain of emotional coercion, constant demands, and social pressure as some of the digital coercion that current evidentiary norms do not adequately address. The law is text-bound, that is, tied to direct verbal or written statements--and digital intercourse is as much conducted with nuanced and multimodal expressions of affect and will. Such a gap between the formalism of law and lived digital realities creates the so-called evidence blindness that Richards and Hartzog define as a situation in which the competitiveness of emotion and platform-design pressures are not acknowledged as such before the law.

The hurdles get further ahead as the harms of privacy are considered in the context of digital intimacy. The ineffectiveness of informational autonomy in the algorithmic era is revealed through non-consensual image distribution, deepfakes, and sextortion. In spite of the fact that the BNS, 2023, is a progressive codification project, which criminalizes a variety of digital and cyber-based harms, its clauses (including that of Section 77) repeats the gendered approach of the previous legislation and does not predict new technologies. The ongoing use of the reactive strategies-post-facto punishment, as opposed to prevention or support, leaves a disjuncture existing between the ideals of law and the application of its practical protection. The Information Technology Act, 2000, and the Digital Personal Data Protection Act, 2023, partially address it but remain under disjointed mandates, meaning that the enforcement agencies lack a consistent procedural directive on how to address technologically complex intimate harms.

Recent enforcement-oriented research by Singh, Pandey and Bajpai indicate that although the BNS and related procedural laws (BNSS, BSA) bring digital evidence processing to date, institutional preparedness remains behind schedule. The state of forensic infrastructure is still immature, and privacy protection is not evenly distributed, which casts some doubts on constitutional proportionality. Researchers tend to encounter the problem of jurisdiction and interpretative uncertainty-especially when it comes to evaluating intention, coercion, or consent when dealing with digital communications cutting across borders. These gaps in operations undermine the effectiveness of legal deterrence despite the ambition of BNS to streamline the justice delivery.

Jurisprudentially and normative wise, the new structures have the dual challenge of being technologically adaptive as well as socially sensitive. The works of Wu, Zhang, and Sylwander endorsing a paradigm of affirmative and iterative digital consent fall into the same camp of relational autonomy theorists. However, making consent digital, Moniz and Mehrnezhad caution, may subject intimate data to a novel risk of surveillance and abuse, which is the ironic datafication of desire. Therefore, traceability and evidentiary clarity are one of the benefits of technology but at the same time, it can compromise the privacy it claims to guard.

Intersectionality and gender inclusiveness have not been resolved yet. Although the BNS may claim to be modernized, researchers such as Bajpai, Gupta, and Shrivastava see inexplicable gender asymmetries and the invisibility of non-binary or male victims. Albeit rhetorically progressive, enforcement remains biased with patriarchy and lack of training to be victim-centred. There is no mention of consent revocation, coercive persuasion and contextual violation of digital trust in the law, further increasing the disparity between normative recognition and experiential justice.

In general, although the Bharatiya Nyaya Sanhita, 2023, represents a step in the direction of digitally aware order of the law in India, it is normatively incomplete regarding addressing the dynamism and relationality of digital consent. What will be most effective is not codified provisions per se but the translation to context sensitive enforcement by

interpretive communities, such as courts, police, and other digital platforms. It would be essential to incorporate technological protection, gender-neutral drafting, and privacy-by-design strategies in enforcement practices to create a legal framework that would help to reconcile the three conflicting needs of autonomy, consent, and protection in digitally mediated intimacy.

POLICY RECOMMENDATION

- Legislative Reforms

Introduce a statute on digital intimacy harms, which is gender-neutral, and expressly criminalizes the non-consensual generation, distribution, or modification of intimate material, such as deepfakes and sextortion, with a standing of 7-10 years imprisonment in the event of a recurrence. Amend BNS Section 77 (voyeurism) and combine with IT Act Sections 66E/67A as to require active platform controls such as hash-matching and 36-hour deepface removal, and align with DPDP Act, 2023, rights to erase data. Implement affirmative digital consent requirements with a successive, revocable affirmation in apps, with tamper-proof logs as a testable standard under Bharatiya Sakshya Adhiniyam (BSA), 2023. .

- Enforcement Enhancements

Create cyber cells in the country, after the example of Cyberdome, in Kerala, where police, ethical hackers, and technological companies train in digital forensics on IP tracking, deepfake identification, and protocols sensitive to the victim. Establish SOPs through Indian Cybercrime Coordination Centre (I4C) to cross-jurisdictional cases, fast-track tribunal to NCII and platform responsibility in order to avoid loss of safe harbor through IT Rules. Choose victim-focused strategies that have psychological support conditions and anti-victim-blaming rules to deal with gendered prejudices.

- Platform and Tech Mandates

Mandate that dating applications and social media enforce watermarking, provenance, and algorithmic audit of any consent features, where failure to comply with this is punishable by a fine of up to 250 crore under DPDP Act. Impose user education on revocable consent and privacy paradoxes with privacy-by-design defaults to limit datafication of intimacy.

- Broader Systemic Measures

Offer judicial training in relational consent structures, also in respect of feminist jurisprudence, and promote community service as a penance of minor offenders in order to cultivate a reformative justice. Find international consensus on EU AI Act on deepfakes norms and monitor the creation of the Digital India Act on evolvable cyber laws. The actions will make BNS a proactive model, which will ensure liberty online.

CONCLUSIONS

This paper shows how radically misleading the traditional paradigm of juridical consent is in the face of the changing realities of digitally mediated intimacy and how Bharatiya Nyaya Sanhita (BNS) is a step in the right direction, though still a step, toward a digital justice paradigm. By overlaying the scholarly publications published since 2023 on the topic of negotiating dynamic consent and privacy datafication and enforcement failures, the study shows that BNS provisions like Section 77 fail to address the issue of relational revocation, AI deepfakes, and platform coercion and, as a result, leads to an evidentiary blindness and gendered biases. The proposed policy revision, such as the positive digital consent legislation and cyber-cells, offer a way to effect change in the legislation, and consequently align the Indian legislation with the feminist theory of relational autonomy, along with the IT Act and DPDP Act.

This argument can further theorize the digital consent concept as an iterative, contextual process rather than a binary phenomenon to weaken the textual explanations and frameworks of evidentiary foundations of the Bharatiya Sakshya Adhiniyam (BSA), 2023. It contributes to comparative jurisprudence, establishing benchmarks of BNS on the other international platforms like the EU AI Act, indicating the provisions of gender-neutral offences and forensic interoperability. The effectiveness of reform in longitudinal case studies should be researched empirically in the future, which can inform the interdisciplinary agendas of AI governance and privacy law as well as victim-centred criminology.

Intimacy digitally mediated runs the risk of reinforcing power structures, with all women and marginalized groups being more susceptible to NCII, sextortion, and algorithmic pressure, which is weakening informational autonomy as validated in Puttaswamy. The social norms of favoring beliefful digital communication and the decrease in the privacy paradox and psychological distress can be changed with the sound implementation of BNS, supported with a sense of platform responsibility

and victim support. Lastly, the reforms would establish a culturally sensitive legal ecosystem safeguarding relational dignity, reduce bias in the enforcement of patriarchy, and promote equal participation in the digital Indian public.

REFERENCES

1. Bharatiya Nyaya Sanhita, 2023 (India), s. 45
2. Bureau of Police Research & Development. Handbook on the Bharatiya Nyaya Sanhita. New Delhi: Bureau of Police Research & Development; 2024
3. Safecity. Section 77 BNS: understanding the law on voyeurism . Safecity Legal Resources; [cited 2026 Jan 24]. Available from: Safecity Legal Resources website.
4. Deb E. Digital consent, deepfakes & revenge porn: confronting non-consensual intimate content. Int J Creat Res Thoughts. 2025;13(4):374. IJCRT25A4447.
5. Ministry of Home Affairs. Stringent action on crime against women [Internet]. PIB Delhi; 2025 Dec 3 [cited 2025 Dec 12]. Available from: https://pib.gov.in
6. Sharma V. Understanding non-consensual dissemination of intimate images laws in India with focus on intermediary liability. NUJS Law Rev. 2021;14(4):1.
7. Shubhi. MeitY introduces SOP mandating 24-hour deadline for takedown of non-consensual intimate imagery . SCC Online Blog; 2025 Nov 12 [cited 2025 Nov 12]
8. Kumari P, Chaudhary S, Das M. Digital privacy at risk: examining India's legal response to the non-consensual sharing of intimate media. Int J Law Soc Sci Stud. 2023;3(3):509-19.
9. Zhu Y. Dating apps and social media: the blurring of boundaries in sexual assault and consent. In: Proceedings of the World Conference on Media and Communication [Internet]. 2025;2(1). Available from: https://doi.org/10.33422/worldcmc.v2i1.1047
10. Patrocino LB, Bevilacqua PD. Autonomy and submission in digital self-exposure and violent exposure of women. Rev Estud Fem. 2023;31(3). Available from: https://doi.org/10.1590/1806-9584-2023v31n384139-en
11. Richards N, Hartzog W. The pathologies of digital consent. Wash Univ Law Rev. 2019;96(6)
12. Evans AE. Negotiating digital sexual consent when sending a nude image [PhD thesis]. Lubbock (TX): Texas Tech University;
13. Zytko D, Furlo N. Online dating as context to design sexual consent technology with women and LGBTQ+ stakeholders. In: Proceedings of the CHI Conference on Human Factors in Computing Systems [Internet]. 2023 Apr. Available from: https://doi.org/10.1145/3544548.3580911
14. Wu H, Zhang W. Digital identity, privacy security, and their legal safeguards in the metaverse. Secur Saf. 2023;2:2023011.
15. Ringmar Sylwander K. Consent in a digital age – rethinking sexting education [Internet]. LSE Politics and Policy Blog; 2025 Jul 31 [cited 2025 Dec 11]. Available from: https://blogs.lse.ac.uk/politicsandpolicy/consent-in-a-digital-age-rethinking-sexting-education/
16. Moniz DP, Mehrnezhad M, Almeida T. Intimate data: exploring perceptions of privacy and privacy-seeking behaviors through the story completion method. In: Human-computer interaction – INTERACT 2023. Lecture Notes in Computer Science. Cham: Springer; 2023. p. 53
17. Wu H, Zhang W. Digital identity, privacy security, and their legal safeguards in the metaverse. Secur Saf. 2023;2:2023011
18. Ringmar Sylwander K. Consent in a digital age – rethinking sexting education [Internet]. LSE Politics and Policy Blog; 2025 Jul 31 [cited 2025 Dec 11]. Available from: https://blogs.lse.ac.uk/politicsandpolicy/consent-in-a-digital-age-rethinking-sexting-education/
19. Moniz DP, Mehrnezhad M, Almeida T. Intimate data: exploring perceptions of privacy and privacy-seeking behaviors through the story completion method. In: Human-computer interaction – INTERACT 2023. Lecture Notes in Computer Science. Cham: Springer; 2023. p. 533. Available from:

https://doi.org/10.1007/978-3-031-42286-7_30

20. Hamilton V, Kaptchuk G, McDonald A, Redmiles EM. Safer digital intimacy for sex workers and beyond: a technical research agenda. IEEE Secur Priv. 2024.
21. Gao S. A study of datafication and digital intimacy on Tinder. Media Commun Res. 2025.
22. Shukla A. From love to leverage: the criminology of revenge porn and digital exploitation. Int J Sci Res Eng Manag. 2025
23. Afrouz R, Vassos S. Adolescents' experiences of cyber-dating abuse and the pattern of abuse through technology: a scoping review. Trauma Violence Abuse. 2024.
24. Draper NA, et al. Privacy resignation, apathy, and cynicism: introduction to a special theme. Big Data Soc. 2024.
25. Amirkhani S, et al. Privacy silence: trust and boundary-setting in mobile phone use within intimate relationships. In: Proceedings of the Extended Abstracts of the CHI Conference on Human Factors in Computing Systems. 2025.
26. Spravtseva K. Psychological aspects of security and privacy in the digital environment. Bull Taras Shevchenko Natl Univ Kyiv Psychol. 2024.
27. Singh S, Pandey S. The evolving cybercrime landscape in India: legal challenges, digital evidence, and new criminal laws. Int J Multidiscip Res. 2025
28. Singh P. Offences against women and children under Bharatiya Nyaya Sanhita. SSRN Electron J. 2024.
29. Naik Y. The Bharatiya Nyaya Sanhita (BNS): a critical examination of India's new penal code. SSRN Electron J. 2024
30. Bajpai M. False promises of marriage as sexual exploitation: evaluating criminal liability under the Bharatiya Nyaya Sanhita, 2023. Int Sci J Eng Manag. 2024.
31. Bajpai A, Gupta A. The imperative of gender neutrality in the Bharatiya Nyaya Sanhita, 2023 and a global comparative examination of gender-neutral laws in sexual offences. Statute Law Rev. 2025.
32. Shrivastava H, Akhter S. A comparative study of the Indian Penal Code and the Bharatiya Nyaya Sanhita's gender-related provisions. Statute Law Rev. 2024.
33. Dixit P. Bhartiya Nyaya Sanhita on sexual offences: a progressive rewrite or unnatural regressive silence. IP Int J Forensic Med Toxicol Sci. 2025.
34. Rizvi NA. The role of law in combatting gender-based violence on social media and online platforms. Int J Multidiscip Res. 2025.

*****