WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Women's Privacy in Cyberspace: An Analysis through the Lens of the Indian Knowledge System, Dignity (Maryada), Consent and Contemporary Digital Rights

Atul Singh[1], Sonali Poddar[2]

[1] Research Scholar, Atal Bihari Vajpayee Vishwavidyalaya, Bilaspur, Chhattisgarh
[2] Assistant professor, kaushlendra Rao Law College, Bilaspur, Chhattisgarh

ABSTRACT :

Indian women are going online faster than ever, yet their privacy is not keeping pace with their online presence. This paper argues that women's privacy in cyberspace is best understood as relational dignity: the capacity to decide who may see, hold, circulate, and speak about one's person, image, and data. It critically engages with the Indian Knowledge System (IKS) as a plural and contested archive that offers real resources (maryada as boundary and dignity, women as knowing subjects, an ethic of reciprocity) alongside real constraints (protection that slides into control). It then examines digital consent, showing that notice-and-consent is structurally weak for women who share devices, navigate unfamiliar languages, and face coercive relationships. Finally, it reviews the constitutional, statutory, and international framework, including the Puttaswamy judgment, the Digital Personal Data Protection Act 2023 and Rules 2025, the Bharatiya Nyaya Sanhita 2023, and the IT Amendment Rules 2026. Official data show sharply rising access (women's internet use rose from 33.3% to 64.3% between NFHS-5 and NFHS-6) and rising cybercrime (86,420 cases in 2023). The paper closes with a Maryada-informed, rights-based framework and actionable recommendations.

Keywords: women's privacy; cyberspace; Indian Knowledge System; maryada; digital consent; DPDP Act 2023; technology-facilitated gender-based violence; intersectionality

1. Introduction

Privacy has long been described as the right to be let alone (Warren & Brandeis, 1890), as control over information about oneself (Westin, 1967), and, more recently, as the appropriate flow of information within particular social contexts (Nissenbaum, 2010). For women in India, each of these ideas is tested daily in cyberspace. The sixth National Family Health Survey (NFHS-6, 2023–24) reports that the share of women aged 15-49 who had ever used the internet nearly doubled, from 33.3% in NFHS-5 to 64.3%, while personal mobile phone use rose from 53.9% to 63.6% (ETV Bharat, 2026; International Institute for Population Sciences [IIPS] & Ministry of Health and Family Welfare [MoHFW], 2021). Connectivity brings education, income, welfare, and sociability. It also brings exposure: the National Crime Records Bureau (NCRB, 2025) recorded 86,420 cybercrime cases in 2023, up 31.2% from 65,893 in 2022.

The topic's significance is therefore both practical and conceptual. Practically, millions of women have become data subjects, content creators, and targets within a few years, often without adequate digital literacy, legal awareness, or control over the devices they use. Conceptually, the Indian privacy debate has been dominated by Western liberal vocabulary and constitutional doctrine, while indigenous moral and philosophical vocabularies (dignity, boundary, duty, reciprocity) are rarely examined for what they can contribute or how they can mislead contemporary digital rights.

Research objectives. The paper (a) examines concepts of privacy, dignity, and autonomy within the Indian Knowledge System, with particular attention to maryada; (b) analyzes the nature and limits of consent in the digital lives of Indian women; (c) reviews national and international digital rights frameworks and the specific harms women face; (d) presents official and institutional data on access and victimization; and (e) proposes recommendations that connect traditional values with contemporary digital needs.

Central argument. Women's cyber-privacy should be grounded in dignity-based autonomy. IKS contributes the idea that dignity is relational and boundary-bearing, and that those with power owe duties of restraint. However, the same tradition has also justified paternalistic "protection" that denies women decisional control. A defensible Maryada-informed approach must therefore retain the first insight and reject the second, anchoring it in the

constitutional promise of privacy as an aspect of dignity and liberty (Justice K. S. Puttaswamy (Retd.) v. Union of India, 2017).

Method and limits. The paper is a doctrinal and secondary-data analysis. It draws on primary legal texts, canonical translations, government statistics, and institutional reports. Official crime statistics capture only reported incidents and almost certainly understate prevalence; survey-based indicators such as "ever used the internet" do not measure frequency or quality of use. Findings should be interpreted with these limits in mind.

Roadmap. Section 2 explores IKS and privacy. Section 3 analyzes consent—Section 4 reviews digital rights and intersectional harms. Section 5 presents data tables and figures. Section 6 discusses case examples. Section 7 offers recommendations, and Section 8 concludes.

2. The Indian Knowledge System and Privacy

2.1 Is there "privacy" in the Indian tradition?

Classical Sanskrit lacks a single word for privacy in the modern informational sense. However, the underlying concerns appear under other terms: the interior self (ātman) that others cannot fully own; the household (gṛha) as a bounded domain; the secret or confidential (guhya, rahasya); and the limits (maryadā) that govern what one may do to or know about another person. Indian legal historians caution against reading modern rights back into ancient texts (Kane, 1930–1962), and Sen (2005) reminds us that the tradition is argumentative and plural, not a single doctrine. This paper therefore treats IKS as a set of interpretive resources, not a code to be applied.

2.2 Maryada: boundary, dignity and restraint

The word maryadā literally denotes a boundary or limit, as of a shore, and extends morally to the proper limits of conduct, propriety, and honor. In popular usage, it often means social honor, frequently attached to women. Read generously, maryada has two aspects relevant to privacy. First, it is a norm of restraint binding the powerful: a person, a ruler, or a community may not cross certain limits when dealing with another. Second, it is a relational, rather than purely individual, idea of dignity: one is standing depends on how others treat one's person and image. The first aspect maps onto the digital duties of platforms, employers, partners, and strangers not to expose, circulate, or manipulate a woman's image and data. The second explains why exposure online is experienced as a violation of standing, not merely a loss of secrecy.

The danger is that Maryada is routinely turned inward onto women, so the burden of maintaining boundaries falls on them (what they wear, post, or reveal) rather than on those who breach them. Feminist legal theory has long warned that "privacy" can shield abuse in the home from scrutiny (MacKinnon, 1989) and that privacy and accountability must be balanced (Allen, 2011). In Indian idiom, the equivalent is the injunction to keep domestic matters within the household. A Maryada-informed privacy must therefore define the boundary as a limit on the intruder, not a veil over the victim.

2.3 Women as knowing subjects

IKS also contains strong evidence of women as speaking, questioning subjects. In the Brihadaranyaka Upanishad, Maitreyi presses Yajnavalkya on the nature of the self and immortality, and Gargi challenges him in public debate (Olivelle, 1998). The *Therigatha* preserves the verses of early Buddhist nuns in their own voices (Hallisey, 2015). These sources matter for privacy because informational self-determination presupposes a subject whose perspective counts. They support the claim that women's decisions about self-presentation and information are their own.

2.4 The ambivalence of the dharmic tradition

The normative texts of the dharma tradition speak with two voices. The Manavadharmashastra declares that where women are honored, the gods are pleased (3.56), yet it also prescribes lifelong guardianship and states that a woman is not fit for independence (9.3) (Olivelle, 2005). Kautilya's Arthashastra devotes sections to women's property and offenses against women, while also treating women's conduct as a matter of social regulation (Olivelle, 2013). Historians have documented how such norms entrenched control over women's sexuality and mobility (Altekar, 1959; Chakravarti, 1989, 2003). The lesson for cyberspace is clear: a "protective" discourse can justify monitoring a woman's phone, restricting her devices, or policing her online presence in the name of honor. That is surveillance, not privacy.

2.5 Reciprocity and the public humiliation of women

The epic tradition offers an ethic of reciprocity, as summarized in the Mahabharata's counsel not to do to others what one finds painful oneself (Anushasana Parva; Debroy, 2010–2014). It also presents a paradigmatic scene of public violation: the assault on Draupadi in the Kuru assembly, where a woman's bodily dignity is attacked before an audience, many of whom remain silent, and where she demands that the assembly answer in terms of dharma (Debroy, 2010–2014; Matilal, 2002). The scene's structure (a public forum, a humiliated woman, passive bystanders, a plea for rules that bind the powerful) closely resembles online shaming and the circulation of intimate or manipulated images. It suggests that bystander complicity and platform inaction are moral failures, not neutral conduct.

Table 1

From IKS concepts to digital-age principles

IKS concept or source	Possible digital-age analog	Caution
Maryada (limit, restraint)	Duty of restraint on platforms and users; purpose limitation and data minimization	Must not become a dress or conduct code for women
Interior self (*ātman*)	Informational self-determination; control over one's profile and images	Metaphysical language cannot substitute for enforceable rights
Women as interlocutors (Maitreyi, Gargi, *Therigatha*)	Women's agency and voice in design, consent and redress	Exemplary figures were exceptional, not typical
Reciprocity (Mahabharata)	Platform and user duty of care; non-consensual sharing as a wrong	Reciprocity is a moral, not legal, standard
Draupadi episode	Bystander and intermediary responsibility; rapid takedown	Epic narrative is illustrative, not evidence
Guardianship norms (Manu 9.3)	Parental and spousal oversight of women's phones	Conflicts with autonomy and with *Puttaswamy*

Note. Compiled by the author from Olivelle (1998, 2005, 2013) and Debroy (2010–2014).

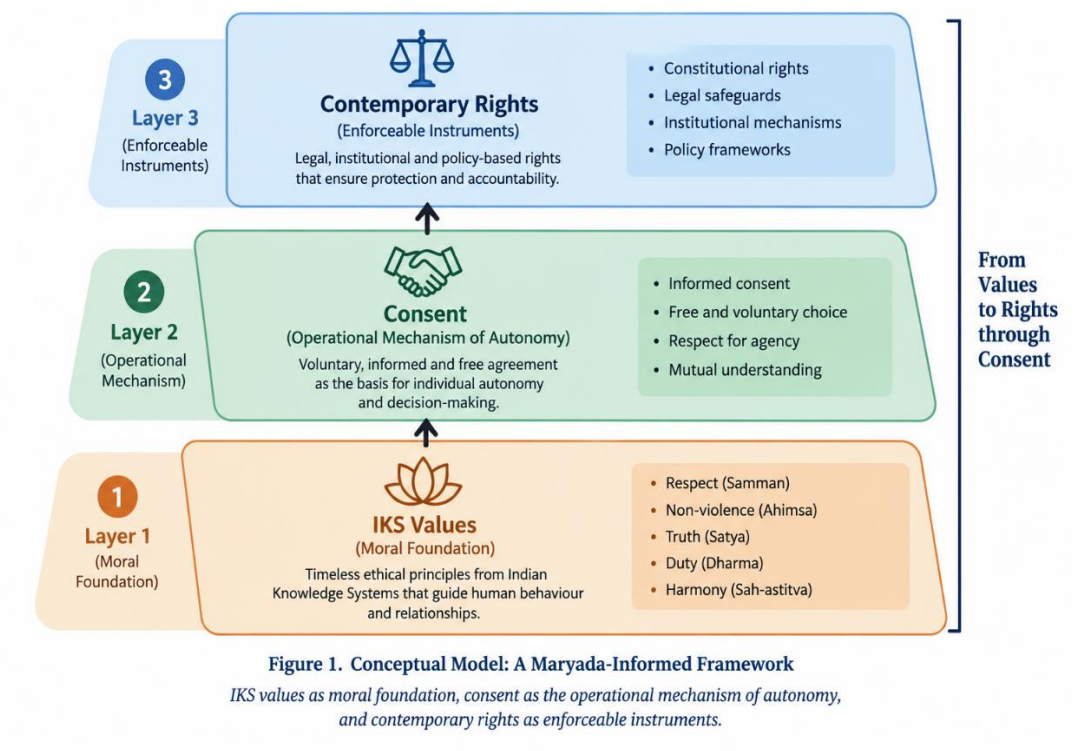


Figure 1. Conceptual Model: A Maryada-Informed Framework

IKS values as moral foundation, consent as the operational mechanism of autonomy, and contemporary rights as enforceable instruments.

3. Consent in the Digital Age

3.1 The consent dilemma

Consent is the cornerstone of most data-protection regimes, yet its practical value is widely doubted. Solove (2013) calls this the consent dilemma: people cannot meaningfully manage the volume and complexity of privacy decisions modern data use requires, yet legal systems keep asking them to. Empirically, reading privacy policies would consume many working days a year (McDonald & Cranor, 2008), and in one experiment nearly all participants joined a fictitious social network without reading its terms, accepting clauses that required surrendering a first-born child (Obar & Oeldorf-Hirsch, 2020). Nissenbaum (2010) adds that consent also misses the point when harm arises from information moving out of its original context, such as a private image shared with one partner that is then posted publicly.

3.2 Why women's consent is more fragile

Several features of Indian women's digital lives weaken the assumption of an informed, free, and individual decision.

- Shared and borrowed devices. The NFHS-6 analysis notes that in several states, internet use does not align with personal phone ownership, suggesting access via shared household devices (Matta, 2026). A woman using a family phone may have no private account space, so consent and privacy settings are effectively negotiated at the household level.
- Language and literacy. Terms and notices are often in English or technical language. The DPDP Act requires notice in English or any language in the Eighth Schedule (Government of India, 2023b), but access to a notice does not equal comprehension.
- Coercive and relational pressure. Consent to share an image or password within an intimate relationship does not constitute consent to further distribution and may be obtained under pressure. Under the contextual integrity view, onward sharing breaches the norms of the original context (Nissenbaum, 2010).
- Public images as "fair game". Photographs women post publicly are routinely scraped and misused. However, data made public by the individual is carved out of the DPDP Act's scope (s. 3(c) (ii)), which may leave a gap for downstream misuse (Government of India, 2023b).
- Proxy consent. When guardians or family members decide what a girl or woman may do online, consent shifts from the data principal to others. The DPDP Rules require verifiable parental consent for individuals under 18 (Ministry of Electronics and Information Technology [MeitY], 2025).

3.3 Consent in the Indian legal framework

The DPDP Act 2023 defines valid consent as free, specific, informed, unconditional, and unambiguous, given by a clear affirmative action, and provides a right to withdraw it as easily as it was given (Government of India, 2023b). It also lists "legitimate uses" for which consent is not required and exempts State instrumentalities in notified circumstances (s. 17). Consent managers, entities registered to help individuals manage permissions, are a new institutional device. The Rules, notified in November 2025, phase in these obligations (MeitY, 2025; AZB & Partners, 2025).

Table 2

Phased commencement of the DPDP Rules, 2025

Phase	Date	What takes effect
I	November (2025).	Data Protection Board provisions and procedures (Rules 1, 2, 17–21)
II	November 2026	Registration and obligations of consent managers (Rule 4)
III	May 2027	Notice, consent, security safeguards, breach notification, children's data and other core duties

Note. Based on MeitY (2025) and AZB & Partners (2025). Dates are approximate to the day of notification and should be verified against the Gazette.

As of October 2026, the core consent obligations for data fiduciaries are not yet in force. Women's consent protection currently rests largely on older provisions (for example, s. 66E of the IT Act on capturing or publishing private images without consent) and on platform terms of service (Government

of India, 2000).

3.4 Implications for e-commerce, social media and apps

In e-commerce and fintech, women's data, such as location, contacts, purchase history, and health information, are collected through bundled permissions. In social media, default public settings and tagging expose images and networks. In dating, health, and period-tracking apps, intimate data carry a high risk of re-identification and misuse. The DPDP framework's purpose-limitation and withdrawal principles address these in theory; in practice, their effectiveness depends on enforcement and on design that treats the woman, not the household, as the data principal.

4. Contemporary Digital Rights and Women

4.1 International frameworks

The Universal Declaration of Human Rights protects against arbitrary interference with privacy, family, home, or correspondence, and against attacks on honor and reputation (United Nations General Assembly [UNGA], 1948, Art. 12). The Convention on the Elimination of All Forms of Discrimination against Women (CEDAW), to which India is a party, is read by the CEDAW Committee (2017) as covering gender-based violence in technology-mediated environments. The UN Special Rapporteur on violence against women (Šimonović, 2018) concluded that online violence must be understood as part of the continuum of gender-based violence and framed within human rights obligations. The EU's General Data Protection Regulation (European Parliament & Council, 2016) offers a comparator with stronger individual rights and a dedicated regulator.

4.2 Constitutional foundations in India

In Justice K. S. Puttaswamy (Retd.) v. Union of India (2017), a nine-judge bench held that privacy is a fundamental right under Articles 14, 19, and 21, encompassing bodily integrity, informational privacy, and decisional autonomy. The judgment links privacy to dignity, a point developed by constitutional scholars (Bhatia, 2019). Other decisions matter for women: Vishaka v. State of Rajasthan (1997) used constitutional values and CEDAW to fill a statutory gap on workplace harassment; Joseph Shine v. Union of India (2019) rejected the notion that a woman is a husband's property and affirmed her dignity and autonomy; and Shreya Singhal v. Union of India (2015) struck down s. 66A of the IT Act and read down intermediary liability to actual knowledge, as determined by court or government orders, a standard now supplemented by faster statutory timelines. The Group of Experts on Privacy (Planning Commission, 2012) and the Srikrishna Committee (2018) laid the policy groundwork for the data protection law.

4.3 Statutory framework

Table 3

Principal Indian legal instruments relevant to women's cyber-privacy

Instrument	Relevant provisions or features	Gap or concern
IT Act, 2000	s. 66E (violation of privacy), ss. 67, 67A, 67B (obscene and sexually explicit material, child material)	Enforcement and proof burdens; limited victim-centered remedies
Bharatiya Nyaya Sanhita, 2023	s. 75 (sexual harassment), s. 77 (voyeurism), s. 78 (stalking, including online), s. 79 (insulting modesty by word, gesture or act intruding on privacy)	Police registration and investigation capacity
DPDP Act, 2023 and Rules, 2025	Consent standard, notice, withdrawal, erasure, grievance redress, consent managers, penalties	Core duties from May 2027; State exemptions (s. 17); public-data carve-out
IT (Intermediary Guidelines) Amendment Rules, 2026	Synthetic content defined and labeled; 3-hour takedown on valid orders; 2-hour window for non-consensual intimate imagery, including deepfake nudity	Operational feasibility; over-removal risk; safe-harbor pressure

Note. Based on the Government of India (2000, 2023a, 2023b), MeitY (2025, 2026), and Bansal (2026). Section numbers should be checked against

current official texts.

The 2026 amendments, notified in February 2026 and effective as of 20 February 2026, bring "synthetically generated information," including deepfakes, within the platform due-diligence regime, require labeling and embedded provenance data, and shorten key takedown windows (MeitY, 2026; Bansal, 2026). They directly address the harm described in the deepfake literature, in which fabricated sexual imagery is used to humiliate and silence women (Chesney & Citron, 2019; Citron, 2019).

4.4 Specific rights challenges

Online harassment and cyberstalking. UN Women (2022) reports that between 16% and 58% of women have experienced technology-facilitated gender-based violence. It cites an Economist Intelligence Unit finding that 38% of women had personal experience of online violence. In comparison, 85% had witnessed it against other women (Economist Intelligence Unit, 2021, as cited in UN Women, 2022). Citron (2014) shows that online abuse of women is also a civil rights problem: it drives women out of public conversation.

Data exploitation. Beyond individual perpetrators, commercial data practices (profiling, targeted advertising, data brokerage) treat women's data as a resource. Sexual privacy, as Citron (2019) argues, deserves distinct protection because of its link to equality and self-development.

Surveillance. State surveillance is permitted through exemptions in the data law; domestic surveillance (a partner or relative monitoring a phone) is socially normalized and rarely framed as a rights violation (Kovacs, 2017). The Maryada critique above applies directly: "protection" is often the stated reason.

Image-based abuse and doxxing. Morphing, non-consensual intimate imagery, and publication of personal details are recurring forms, discussed in the Indian cyber-victimization literature (Halder & Jaishankar, 2012).

4.5 Intersectionality, technology and power

Crenshaw (1991) showed that violence against women is experienced differently at the intersection of gender with race and class. In India, caste, religion, region and class shape both access and risk. Amnesty International India's (2020) analysis of 114,716 tweets mentioning 95 women politicians found that 13.8% were problematic or abusive (10.5% problematic, 3.3% abusive), roughly double the 7.1% found in a similar UK and US study, and reported that Muslim women politicians received 94.1% more ethnic or religious slurs and women from marginalized castes received 59% more caste-based abuse than others. Digital power is also unevenly distributed in access: urban women's internet use stood at 77.3% versus 58.6% for rural women in NFHS-6 (Matta, 2026). Privacy laws that treat "women" as one category will miss these gradients.

5. Data Analysis and Visual Representation

5.1 Access is expanding quickly but unevenly

Women's connectivity has changed faster than most privacy protections. Between NFHS-5 (2019–21) and NFHS-6 (2023–24), the share of women aged 15–49 who had ever used the internet rose from 33.3% to 64.3%, while the urban–rural gap persisted (Table 4). Personal phone use of 63.6% means more than one in three women still has no phone she uses herself, consistent with the shared-device pattern noted in Section 3.

Table 4

Women's digital and financial access, India (women aged 15-49, %)

Indicator	NFHS-5 (2019–21)	NFHS-6 (2023–24)
Ever used the internet	33.3	64.3
Urban women	51.8	77.3
Rural women	24.6	58.6
Have a mobile phone they themselves use	53.9	63.6
Have a bank or savings account they themselves use	78.6	89.0

Note. Data from ETV Bharat (2026). Matta (2026) and IIPS & MoHFW (2021). "Ever used the internet" does not measure frequency or independence of use.

5.2 Reported victimization is rising

NCRB data show that registered cybercrime grew every year from 2020 to 2023 (Table 5). Most registered cases are fraud, but women-specific heads are also growing. For women, publication or transmission of sexually explicit material rose from 1,896 cases in 2021 to 2,251 in 2022, while blackmail, defamation, morphing, and fake-profile offenses were 701 and 689 in the same years (Rajkumar, 2023). NCRB data for 2023 show 2,767 cases under cyber pornography and obscene sexual material and 1,358 under cyber stalking and bullying of women (Dataful, n.d.); head definitions can differ across years, so these are indicative rather than strictly comparable.

Table 5

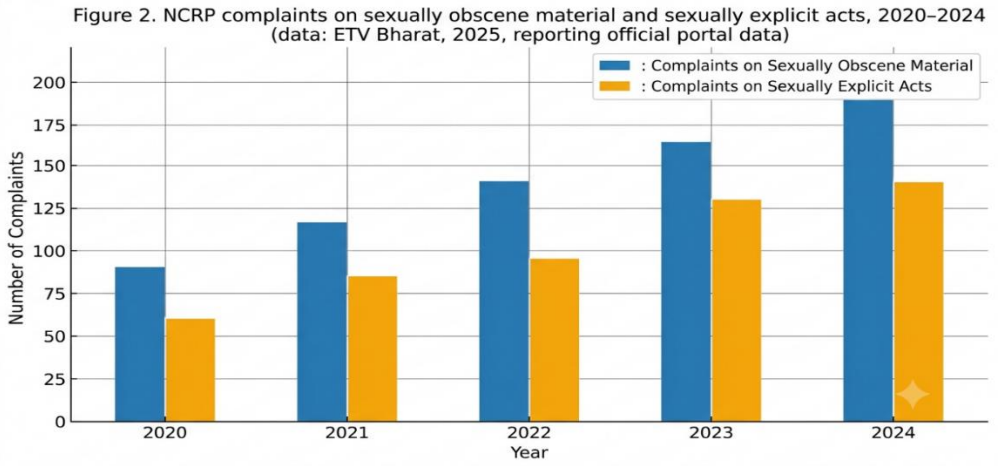
Cybercrime cases registered in India, 2020–2023

Year	Cases registered	Change on previous year
2020	50,035	—
2021	52,974	+5.9%
2022	65,893	+24.4%
2023	86,420	+31.2%

Note. Data from the Ministry of Home Affairs (2023) for 2020–2022 and NCRB (2025) for 2023.

Enforcement lags registration. Cases ending in conviction under cybercrime heads were 1,110 in 2020, 491 in 2021 and 1,118 in 2022 (Ministry of Home Affairs, 2023), a small fraction of registered cases in each year. However, convictions in a year relate to cases registered earlier. Complaints made directly on the National Cyber Crime Reporting Portal (NCRP) give a fuller picture of the demand for redress. Complaints about sexually obscene material and sexually explicit acts rose from 17,985 in 2020 to 38,123 in 2024 (ETV Bharat, 2025), as shown in Figure 2.

Figure 2. NCRP complaints on sexually obscene material and sexually explicit acts, 2020–2024 (data: ETV Bharat, 2025, reporting official portal data)



5.3 Reading the data together

- **Exposure follows access.** As more women go online, more of their images and data become available to misuse, while many still lack a private device or space.
- **Registered cases understate harm.** Survey-based studies report far higher prevalence of technology-facilitated violence (16–58% globally; UN Women, 2022) than administrative counts suggest, and women often avoid reporting because of stigma and the very honor norms discussed in Section 2.
- **Redress is slow relative to harm.** Content spreads in minutes; conviction takes years. The 2026 takedown windows address speed, but not the investigation and prosecution gap.

6. Case Studies and Examples

6.1 Case 1: Online "auction" apps targeting Muslim women (2021–2022)

In July 2021, an app called "Sulli Deals", hosted on the open-source platform GitHub, displayed photographs and social media profiles of more than 80 Muslim women as "deals of the day"; in January 2022, a similar app, "Bulli Bai", listed more than 100 women, many of them journalists, lawyers and activists (Global Voices, 2022). The women's photographs had been taken from their public social media accounts without consent. Police in Mumbai and Delhi made arrests in early January 2022, including the person alleged to have created the first app, who was arrested only after the second app emerged (Al Jazeera, 2022).

The case illustrates five points of the analysis. First, consent was absent at every stage: collection, compilation, and publication. Second, publicly posted images are not "public property", yet the DPDP Act's carve-out for data made public by the individual leaves a gap that legal remedies must fill through other offenses. Third, the targeting combined gender with religion, an intersectional harm of the kind Crenshaw (1991) describes and Amnesty International India (2020) documents. Fourth, a platform's hosting and removal practices were central, which is why intermediary timelines were faster. Fifth, in terms of maryada, the "auction" is a deliberate public humiliation, echoing the Draupadi episode in structure: a woman displayed before an audience for the pleasure of her tormentors.

6.2 Case 2 (illustrative composite): The shared phone and the loan app

The author constructed the following vignette from patterns discussed in the literature; it is not a report of a specific person. A young woman in a small town uses her brother's phone. To obtain a small loan, she installs an app that requests access to contacts and photographs, and she accepts without reading the permissions, which are in English. After she misses a repayment, the lender threatens to send edited images to her contacts. She does not report it, fearing that her family will restrict her phone use and blame her for the exposure.

Every weakness identified in Section 3 appears here: bundled consent, language barrier, shared device, proxy control and fear of honor-based blame. The legal tools exist (IT Act s. 66E, BNS ss. 77–79, the DPDP Act's purpose-limitation rules once in force), but social rather than legal barriers block the woman's route to them.

7. Future Suggestions and Recommendations

The most durable protection for women's privacy combines design, law, education and community action, and rests on one principle drawn from the Maryada tradition: limits bind the intruder, not the victim. Table 6 sets out recommendations by domain.

Table 6
Recommendations for strengthening women's privacy in cyberspace

Domain	Recommendation	Rationale and link to IKS
Technology	Privacy-by-default settings for new accounts (private profile, limited tagging, hidden contact discovery); hash-based blocking of reported intimate images across platforms; shared-device or guest profiles; icon-based, audio and local-language consent notices	Reduces dependence on reading policies (Solove, 2013); treats the woman, not the household, as the data principal; builds restraint into design
Policy	Operationalize the DPDP Act before May 2027 with gender-sensitive consent-manager standards; confine State exemptions under s. 17 to necessity and proportionality; review the carve-out for publicly posted data	Consistent with the proportionality reasoning in *Puttaswamy* (2017); closes the scraping gap seen in Case 1
Legal reform	A clear offense and fast civil remedy for non-consensual synthetic intimate imagery; victim anonymity and trauma-informed procedure; consequences for repeated intermediary non-compliance; women-staffed cyber-crime desks	Moves enforcement from speed of takedown to accountability; responds to sexual-privacy harms (Citron, 2019)
Education	Digital literacy in Indian languages for women and girls; school modules on consent, image-based abuse and bystander duty; training for police, prosecutors and judges	Treats women as knowing subjects, in the spirit of Maitreyi and Gargi (Olivelle, 1998)
Community	Panchayats, self-help-group federations and frontline health and child-care	Uses existing local institutions without

	workers as trusted awareness and reporting points; peer "digital volunteers"	reproducing guardianship norms
Research and data	Disaggregate cybercrime data by victim age, caste and religion; periodic national prevalence surveys on technology-facilitated violence; independent audits of takedown timelines	Makes intersectional harm (Crenshaw, 1991) visible to policy

Note. Compiled by the author.

Bridging traditional values and digital needs

Three principles can carry IKS ideas into digital governance without importing its constraints. First, **reassign maryada**: public campaigns and platform codes should present boundary-keeping as the obligation of those who view, share, and profit from images and data, and avoid any language of modesty directed at women. Second, **replace guardianship with accompaniment**: families can support a woman's digital life through conversation and trusted reporting, not by monitoring her phone, which the data and law treat as an intrusion on her autonomy (*Puttaswamy*, 2017; Kovacs, 2017). Third, **make reciprocity a duty of care**: the epic ethic of not doing to others what one finds painful (Debroy, 2010–2014) can anchor bystander norms and platform responsibility, and narratives such as the Draupadi episode can be used in awareness work to make the bystander's role visible.

8. Conclusion

Women's privacy in cyberspace is a question of dignity before it is a question of data. The evidence reviewed here shows rapid growth in women's access (33.3% to 64.3% internet use between NFHS-5 and NFHS-6), steeply rising registered cybercrime (86,420 cases in 2023), and a protective framework that is stronger than before but incomplete: the DPDP Act's core consent duties apply only from 2027, State exemptions and the public-data carve-out leave gaps, and enforcement trails harm.

The Indian Knowledge System contributes a valuable idea: dignity is relational, and limits bind the powerful, along with a warning that "protection" can become control. A Maryada-informed approach keeps the first and rejects the second, and fits with the constitutional recognition of privacy as part of dignity and liberty. Consent must be redesigned for the realities of shared devices, language barriers and relational pressure, and rights must be read intersectionally.

The future of women's privacy in India will depend less on a single statute than on whether platforms, institutions, families and communities accept the duty of restraint, and whether women are treated as the authors of their own digital lives. Further empirical work, especially national prevalence data and studies of how women themselves experience consent and redress, is needed to test and refine the framework offered here.

REFERENCES

- Al Jazeera. (2022, January 5). *India police make arrests in online "auction" of Muslim women*. https://www.aljazeera.com/news/2022/1/5/india-police-arrests-bulli-bai-online-auction-muslim-women
- Allen, A. L. (2011). *Unpopular privacy: What must we hide?* Oxford University Press.
- Altekar, A. S. (1959). *The position of women in Hindu civilization: From prehistoric times to the present day* (2nd ed.). Motilal Banarsidass.
- Amnesty International India. (2020). *Troll Patrol India: Exposing online abuse faced by women politicians in India*. Indians for Amnesty International Trust.
- AZB & Partners. (2025, November 19). *Update – India's Digital Personal Data Protection framework comes into effect*. https://www.azbpartners.com/bank/update-indias-digital-personal-data-protection-framework-comes-into-effect/
- Bansal, A. (2026, February 10). *MeitY notifies new amendments to IT Rules to regulate synthetic media and deepfakes*. MediaNama. https://www.medianama.com/2026/02/223-meity-amendments-it-rules-synthetic-media-deepfakes/
- Bhatia, G. (2019). *The transformative Constitution: A radical biography in nine acts*. HarperCollins India.
- CEDAW Committee. (2017). *General Recommendation No. 35 on gender-based violence against women, updating General Recommendation No. 19* (CEDAW/C/GC/35). United Nations.
- Chakravarti, U. (1989). Whatever happened to the Vedic *dasi*? Orientalism, nationalism and a script for the past. In K. Sangari & S. Vaid (Eds.), *Recasting women: Essays in colonial history* (pp. 27–87). Kali for Women.

- Chakravarti, U. (2003). *Gendering caste: Through a feminist lens*. Stree.
- Chesney, R., & Citron, D. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review, 107*(6), 1753–1819.
- Citron, D. K. (2014). *Hate crimes in cyberspace*. Harvard University Press.
- Citron, D. K. (2019). Sexual privacy. *Yale Law Journal, 128*(7), 1870–1960.
- Crenshaw, K. (1991). Mapping the margins: Intersectionality, identity politics, and violence against women of color. *Stanford Law Review, 43*(6), 1241–1299.
- Dataful. (n.d.). *NCRB – Cyber crimes: Year and crime head-wise number of cyber crimes committed against women in India* [Data set]. https://dataful.in/datasets/22356
- Debroy, B. (Trans.). (2010–2014). *The Mahabharata* (Vols. 1–10). Penguin Books India.
- ETV Bharat. (2025, March 19). *2,25,001 cybercrime incidents related to crimes against women registered in the last five years*. https://www.etvbharat.com/en/!bharat/cybercrime-incidents-related-to-crimes-against-women-enn25031904757
- ETV Bharat. (2026, May 30). *Women using the internet nearly doubled in India, finds NFHS-6*. https://www.etvbharat.com/en/bharat/women-using-internet-nearly-doubled-in-india-finds-nfhs-6-enn26053000977
- European Parliament & Council of the European Union. (2016). Regulation (EU) 2016/679 on the protection of natural persons about the processing of personal data (General Data Protection Regulation). *Official Journal of the European Union, L 119*, 1–88.
- Global Voices. (2022, January 17). *Bulli Bai, Sulli Deals cases highlight rising communal misogyny in India*. https://globalvoices.org/2022/01/17/bulli-bai-sulli-deals-cases-highlight-rising-communal-misogyny-in-india/
- Government of India. (2000). *The Information Technology Act, 2000* (Act No. 21 of 2000).
- Government of India. (2023a). *The Bharatiya Nyaya Sanhita, 2023* (Act No. 45 of 2023).
- Government of India. (2023b). *The Digital Personal Data Protection Act, 2023* (Act No. 22 of 2023).
- Halder, D., & Jaishankar, K. (2012). *Cyber crime and the victimization of women: Laws, rights and regulations*. IGI Global.
- Hallisey, C. (Trans.). (2015). *Therigatha: Poems of the first Buddhist women*. Harvard University Press.
- International Institute for Population Sciences & Ministry of Health and Family Welfare. (2021). *National Family Health Survey (NFHS-5), 2019–21: India*. IIPS.
- *Joseph Shine v. Union of India*, (2019) 3 SCC 39.
- *Justice K. S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
- Kane, P. V. (1930–1962). *History of Dharmaśāstra* (Vols. 1–5). Bhandarkar Oriental Research Institute.
- Kovacs, A. (2017). *Reading surveillance through a gendered lens: Some theory*. Internet Democracy Project.
- MacKinnon, C. A. (1989). *Toward a feminist theory of the state*. Harvard University Press.
- Matilal, B. K. (2002). *Ethics and epics: Philosophy, culture and religion* (J. Ganeri, Ed.). Oxford University Press.
- Matta, A. (2026, July 3). *Women's internet use nearly doubles, but access gaps remain*. Dataful Insights. https://insights.dataful.in/articles/womens-internet-use-nearly-doubles-but-access-gaps-remain
- McDonald, A. M., & Cranor, L. F. (2008). The cost of reading privacy policies. *I/S: A Journal of Law and Policy for the Information Society, 4*(3), 543–568.
- Ministry of Electronics and Information Technology. (2025). *Digital Personal Data Protection Rules, 2025* [Gazette notification]. Government of India.
- Ministry of Electronics and Information Technology. (2026). *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026* (G.S.R. 120(E)). Government of India.
- Ministry of Home Affairs. (2023, December 20). *Cyber crimes in India* [Reply to Rajya Sabha unstarred question]. Rajya Sabha Secretariat. https://rsdebate.nic.in/bitstream/123456789/745565/1/PQ_262_20122023_U1979_p233_p235.pdf
- National Crime Records Bureau. (2025). *Crime in India 2023*. Ministry of Home Affairs, Government of India.
- Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.
- Obar, J. A., & Oeldorf-Hirsch, A. (2020). The biggest lie on the Internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society, 23*(1), 128–147.
- Olivelle, P. (Trans.). (1998). *The early Upaniṣads: Annotated text and translation*. Oxford University Press.
- Olivelle, P. (Trans.). (2005). *Manu's code of law: A critical edition and translation of the Mānavadharmaśāstra*. Oxford University Press.
- Olivelle, P. (Trans.). (2013). *King, governance, and law in ancient India: Kauṭilya's Arthashāstra*. Oxford University Press.
- Planning Commission. (2012). *Report of the Group of Experts on Privacy* (Chair: A. P. Shah)—Government of India.

- Rajkumar, A. (2023, December 4). *Crimes against women rise by 4%, cyber crimes increase by 11%: NCRB data*. The News Minute. https://www.thenewsminute.com/news/crimes-against-women-rise-by-4-cyber-crimes-increase-by-11-ncrb-data
- Sen, A. (2005). *The argumentative Indian: Writings on Indian history, culture and identity*. Allen Lane.
- *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.
- Šimonović, D. (2018). *Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective* (A/HRC/38/47). United Nations Human Rights Council.
- Solove, D. J. (2013). Introduction: Privacy self-management and the consent dilemma. *Harvard Law Review, 126*(7), 1880–1903.
- Srikrishna Committee. (2018). *A free and fair digital economy: Protecting privacy, empowering Indians*. Ministry of Electronics and Information Technology.
- United Nations General Assembly. (1948). *Universal Declaration of Human Rights* (Resolution 217 A).
- UN Women. (2022). *Accelerating efforts to tackle online and technology-facilitated violence against women and girls*. https://www.unwomen.org/en/what-we-do/ending-violence-against-women/faqs/tech-facilitated-gender-based-violence
- *Vishaka v. State of Rajasthan*, AIR 1997 SC 3011.
- Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review, 4*(5), 193–220.
- Westin, A. F. (1967). *Privacy and freedom*. Atheneum.