



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2025

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

THE GAPS IN INDIAN CYBER LAW: A POLICY FRAMEWORK FOR PROTECTING DIGITAL INTIMACY RIGHTS

~ Pia Chopra

In today's hyper-connected world, love, friendship and yes, digital intimacy often travel through the massive web we call cyberspace. They're faster than a shy "seen" message on WhatsApp. However, while technology has dipped its toes into the intimate corners of our lives, the Indian cyber law is still trying to catch up without tripping over its own limitations that are like wires around its constitution. When it comes to protecting digital intimacy rights such as those against the negative use of private photos, consensual relationships online and sensitive personal data, the Indian legal landscape in India unfortunately turns into a smartphone running on low battery, which means, it is promising but is struggling to rather keep up. So, what is really going on, and how do we fix this conundrum of digital intimacy?

THE CURRENT LEGAL FRAMEWORK: BITS AND PIECES, BUT NO WHOLE PICTURE

India has made some strides with its landmark Information Technology Act, 2000 (IT Act), the India Penal Code (IPC), and, more recently, the Digital Personal Data Protection Act (DPDP) 2023. These laws definitely form the backbone of cyberlaw protections. Some examples to prove the same are- IT Act's Section 66E which criminalizes capturing or sharing the private images of a person without consent, while Section 67A punishes the electronic transmission of sexually explicit content. Meanwhile, the IPC's Section 354C addresses voyeurism which is mainly focused on women's privacy in "private acts."

While this might sound viable in theory, but in practice? Not so much. These laws are reactive and fragmented because they don't anticipate the fast, anonymous and viral nature of digital content spreading across social media and messaging apps. Even worse, they hinge heavily on outdated definitions like "private acts" meaning only certain scenarios, which courts have, at times, interpreted narrowly. Furthermore, the IPC's voyeurism law applies only to women, thereby leaving a significant gap concerning men and non-binary individuals/those belonging to the LGBTQ+ community.

DIGITAL INTIMACY IN DANGER: FROM IMAGE-BASED ABUSE TO DEEPPAKES

The rise of image-based abuse such as non-consensual sharing of intimate photos or videos is a nightmare that many face but only a handful of laws fully protect against. Add to that a new issue right around the corner: deepfakes and AI-generated synthetic intimate content. India's laws barely touch this emerging threat and the current IT rules also lack mandatory timelines for platform takedowns and don't enforce swift hash-matching in order to block the re-uploads, which means that the intimate content keeps on haunting the victims endlessly.

WOES OF ENFORCEMENT: THE SILENCE OF CYBER LAMBS

Practice and theory, scenarios and real-life incidents quite differ from each other. Victims often stumble upon one of the biggest hurdles: Whether they should report the crime or not. Most are unaware of the existence of appropriate legal channels such as National Cybercrime Reporting Portal or even which laws to invoke. When the complaints are filed, the police officers are also subject to bias who often dismiss these cases as "private matters", or worse, blame the victim. This "offline bias" arises because many law enforcers lack empathy and education about being digital savvy to handle online privacy violations effectively. Even the digital forensic capabilities are often missing in local police stations thereby, making it tough to trace the perpetrators or enforce timely takedowns.

Other than that, on the platform side, the Indian cyber law currently does not hold social media companies and their intermediaries as adequately accountable for proactive content moderation, thus, contributing further to the frustration of the victim.

PRIVACY, CONSENT AND DPDP

The advent of the Digital Personal Data Protection Act, 2023 (DPDP Act) offers a glimmer of hope. It enshrines several individual rights like consent, data protection, erasure while also including the creation of a Data Protection Board to oversee compliance. The new act emphasizes data minimisation and lawful purpose in data processing and promotes data localization to enhance security.

However, transitioning from legislation on paper to real empowerment remains a slow and bumpy ride. Public awareness is low, enforcement mechanisms are in early stages, and robust regulatory frameworks for AI and emerging technologies remain absent. The DPDP Act's protections need to be coupled with strong, victim-centric implementation and education to make a genuine difference.

WAY FORWARD: A BETTER POLICY FRAMEWORK

The question that persists now is how do we get from here to a future that really protects digital intimacy of the citizens of the country? This can be done through several provisions like creating a unified, gender-neutral legislation thereby, embracing a comprehensive definition of intimate digital acts including non-consensual sharing and AI-altered content, thus, covering all the victims equally. There shall also be mandatory platform accountability on social media and messaging apps and hosting services need clear obligations for timely content takedown, and hash-matching technology to prevent the repeated abuse and ensure transparent reporting mechanisms.

There should also be an establishment of specialised cybercrime units with trained personnel who are sensitive to issues of digital intimacies in order to remove offline-bias. Other than this, regular training should also be conducted in order to improve technological literacy, empathy and handling of online intimacy cases with rapid and meticulous responses while also promoting large-scale public awareness and prevention of such issues from occurring. However, the most important of all is that these legal provisions should be adaptive. Laws should be able to anticipate and regulate the threats from AI, deepfakes and synthetic media proactively and rather than suffering with weak frameworks, they should be able to catch the perpetrators swiftly.

THE FINAL WORD

Digital intimacy is more than just private pictures or texts; it involves dignity, autonomy, and trust in the digital age. When laws fall behind, victims experience not only psychological harm but also reputational damage and societal stigma, especially in India's complex social environment. Without strong legal and social support, digital intimacy risks becoming one of the most vulnerable areas for human rights violations. Indian cyber law is at a turning point. The digital revolution has opened the door to new forms of intimacy and, unfortunately, new forms of violations. The mix of existing laws, enforcement gaps, and emerging technology challenges means that rights related to digital intimacy often remain uncertain.

However, with the Digital Personal Data Protection Act 2023 and increasing public discussion, a new beginning is possible. This could lead to a situation where rights are honoured, privacy is safeguarded, and digital intimacy can flourish safely. Until then, the key message is clear: adapt or get left behind.

REFERENCES

1. Kumari, P., Chaudhary, S., & Das, M., Digital Privacy At Risk: Examining India's Legal Response to the Non-Consensual Sharing of Intimate Media, Indian Journal of Law and Social Sciences (2025),
<https://ijlsss.com/digital-privacy-at-risk-examining-indias-legal-response-to-the-non-consensual-sharing-of-intimate-media/>
2. Ministry of Electronics and Information Technology, Government of India, The Digital Personal Data Protection Act, 2023 (Aug. 11, 2023),
<https://www.meity.gov.in/static/uploads/2024/06/2bflf0e9f04e6fb4f8fef35e82c42aa5.pdf>.
3. Privacy World, The Impact of India's New Digital Personal Data Protection Rules (Aug. 3, 2025),

<https://www.privacyworld.blog/2025/04/the-impact-of-indias-new-digital-personal-data-protection-rules/>.

4. Centre for Law and Policy Research, Understanding Virtual/Digital Rape: Navigating Consent and Accountability in the Digital Age (Feb. 9, 2025),
<https://clpr.org.in/blog/understanding-virtual-digital-rape-navigating-consent-and-accountability-in-the-digital-age/>.
5. InCountry, Comprehensive Guide to Indian Data Privacy Laws (Dec. 1, 2024),
<https://incountry.com/blog/comprehensive-guide-to-indian-data-privacy-laws/>.
6. PRS India, The Digital Personal Data Protection Bill, 2023 (Sept. 27, 2025),
<https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023>.
7. DLA Piper, Data Protection Laws in India (Apr. 29, 2024),
<https://www.dlapiperdataprotection.com/?t=law&c=IN>.