



JOURNAL OF CYBER GOVERNANCE AND INTELLECTUAL PROPERTY

Volume 1, Issue 2

Article 7

Online Dating Applications and User Safety: Examining the Emerging Legal and Regulatory Framework

Ritisha Jeeda

Thakur Ramnarayan College of Law, Dahisar East, Affiliated to Mumbai University

Recommended Citation:

Jeeda (2026) "Online Dating Applications and User Safety: Examining the Emerging Legal and Regulatory Framework" Journal of Cyber Governance and Intellectual Property, Vol. 1, Issue 2, Article 7. (DOI)

This article is published under the Creative Commons Attribution–NonCommercial–ShareAlike 4.0 International (CC BY-NC-SA 4.0) License, which allows for free non-commercial use, distribution, and reproduction in any medium, provided appropriate credit is given to the original work.

ABSTRACT

Modern relationships have been transformed by the introduction of online dating applications, by enabling rapid, location-based, and algorithm-driven connections, but they have also generated significant risks to user safety, privacy and dignity. This paper examines the legal challenges posed by dating apps, with particular attention to harassment, stalking, impersonation, fraud, non-consensual sharing of intimate images, data misuse, and the inadequacy of platform accountability mechanisms. It adopts a short, comparative approach, analysing Indian law alongside selected international legal frameworks to assess how different jurisdictions regulate intermediary responsibility, online safety, consent, and personal data protection. In the Indian context, the study considers the Digital Personal Data Protection Act, 2023, the Information Technology Act, 2000, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, and other relevant criminal law protections dealing with cyber harassment and sexual offences. The paper argues that while existing laws provide a partial basis for redress, they are not fully adapted to the specific risks created by dating-app environments, where anonymity, speed of contact, and data-intensive design intensify harm. It concludes by suggesting that a more effective legal framework must combine privacy protection, safer platform design, stronger grievance redressal, and clearer intermediary accountability to better protect users in digital intimate spaces.

KEYWORDS

Online Dating, User Safety, Digital Privacy, Intermediary Liability, Data Protection.

INTRODUCTION

Online dating apps have become a routine part of social interaction in India, reshaping the way individuals communicate, form relationships, and negotiate intimacy in digital spaces. At the same time, these platforms have created new and serious user safety concerns, including stalking, impersonation, coercion, non-consensual sharing of intimate images, data misuse, fraud, and online sexual harassment. From a legal perspective, this makes dating applications a useful site for examining the limits of existing Indian law, because the harms that arise on these platforms often intersect at privacy, intermediary liability, criminal law, and data protection. The Digital Personal Data Protection Act, 2023, recognises the importance of lawful processing, consent and grievance redressal in relation to digital personal data¹. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, also impose due diligence obligations on intermediaries, requiring grievance redressal mechanisms, and specifically address unlawful, obscene, and privacy-invasive content, including complaints involving nudity, sexual conduct, and impersonation². These show that Indian law increasingly acknowledges platform responsibility, yet the practical protection available to users of dating apps remains uneven and fragmented.

A legal analysis of online dating app safety must, therefore, move beyond individual crimes and ask how far platform structure, content moderation practices, and data governance rules can prevent harm before it occurs. Dating apps collect highly sensitive behavioural and location-based information, making informed consent, data minimisation, and security safeguards important for user protection. They also give boost to offences already recognised under Indian law, including cyber-enabled harassment and privacy violations, while intermediary rules require platforms to act against unlawful content and assist authorised agencies where necessary. The challenge is that many dating-app harms are difficult to classify, prove, or remedy once they occur, especially where users face anonymity, cross-border actors, or delayed platform response. This paper, therefore, examines whether India's current legal framework adequately protects dating-app users, and whether stronger

¹ The Digital Personal Data Protection Act, 2023 (no. 22 of 2023), <https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf> (last visited Jul 14, 2026).

² The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 1, <https://www.meity.gov.in/static/uploads/2024/02/Information-Technology-Intermediary-Guidelines-and-Digital-Media-Ethics-Code-Rules-2021-updated-06.04.2023-.pdf> (last visited July 14, 2026).

safety-by-design duties, clearer reporting obligations, and more effective redress mechanisms are needed to balance autonomy, innovation, and dignity in online intimate spaces.

LITERATURE REVIEW

Understanding how online dating evolved will help explain why user safety has become such a pressing issue. Early efforts to find a life partner relied on personal ads, and later, computer-assisted matching systems, which were slow, limited and mediated by scarce information. The commercial internet expanded this model through platforms such as match.com in the 1990s³, and mobile apps later drove the process through geolocation and interfaces where you could swipe left and right to accept or reject matches. Tinder and Grindr are often treated as crucial points because they make matching faster and more casual, while also increasing exposure to unwanted contact, deception, and abuse.

A large part of criminology and cyber-safety literature focuses on harms that arise specifically in dating-app environments like stalking, coercion, sexual violence, image-based abuse, blackmail and financial scams, often facilitated by anonymity, rapid messaging, and weak identity verification. Current regulatory frameworks reflect these concerns. In the Indian context, the legal framework remains anchored primarily in the IT Act, 2000 and the IT Rules, 2021. The Digital Personal Data Protection Act, 2023, adds a separate layer of accountability by regulating lawful processing, consent and user rights in relation to digital personal data. Together, these Acts partially talk about liability and compliance, but they do not explicitly address the unique risk profile of dating apps, where intimate disclosure, geolocation, and profile-based matching create distinct safety concerns.

Legal papers on platform responsibility have begun to ask whether dating-service providers should owe users a duty of care, and if so, how that duty should be framed⁴. Some writers argue that negligence principles may apply where harms are foreseeable and platforms fail to adopt reasonable safeguards; others explore whether product liability or consumer protection doctrines can better capture harms caused by design choices, misleading safety claims, or inadequate moderation. The literature also suggests research gaps. A lot of the existing work

³ Pratyusha Pal, *Emergence of online dating apps & its psychological impact*, 26 IJPS 8 (2024), <https://www.psychologyjournal.net/archives/2024/vol6issue1/PartA/6-1-3-372.pdf> (last visited July 14, 2026).

⁴ O'Brien, C.R., Roslan, N.A., Murdoch, S.J., Abu-Salma, R., Zytka, D. and Warner, M., 2025, April. Online Dating Platform Safeguards and Self-Protection: How Dating Platforms Characterise, Respond to, and Safeguard Against Harms. In *Proceedings of the Extended Abstracts of the CHI Conference on Human Factors in Computing Systems* (pp. 1-8).

is concentrated in psychology, criminology, and public-health, while doctrinal, legal analysis of dating-app-specific liability, especially under cybersecurity laws, remains limited, especially in India. There is little systematic discussion of cases that test concepts such as foreseeability, consent, causation, and allocation of risk. Indian scholarship in particular has not yet fully examined whether intermediary liability rules, consumer law, data protection law, and criminal law together form a coherent framework for dating-app harms. This gap justifies a look into whether existing law can adequately protect users or whether dating platforms require a more explicit safety-based legal regime.

RESEARCH METHODOLOGY

This paper uses a doctrinal legal methodology to study online dating apps and user safety. The doctrinal component analyses the relevant statutory framework, subordinate legislation, platform terms of service, judicial decisions, and other regulatory materials to determine how Indian law addresses online harms, intermediary responsibility, privacy and remedies available to users.

The doctrinal inquiry focuses on the legal structure that governs online platform harms in India, including the IT Act, 2000, the IT Rules, 2021, the DPDP Act, 2023, and other relevant criminal law provisions dealing with stalking, sexual violence, fraud, intimidation, and image-based abuse. The paper also examines consumer-protection principles where platform representations about safety, verification, moderation, or reporting tools may create legal expectations. In addition, platform terms of service, community guidelines, and safety policies are reviewed because they shape the practical allocation of responsibility between users and platforms.

The study relies on both primary and secondary sources. Primary sources include statutes, rules, government notifications, official guidance notes, reported judgements, tribunal decisions, and platform policies. Secondary sources include law review articles, policy reports, consultation papers, and scholarship on online safety, platform governance, intermediary liability, and dating-app harms. These materials are used to understand how scholars and regulators conceptualize dating-app safety and whether existing legal categories capture the harms at hand.

ORIGIN OF DATING APPLICATIONS

Since time immemorial, one thing humanity has always accepted has been the duty of homo sapiens as a species to reproduce. The concept of reproduction, familial institutions, marriage, and love has been through several, notable changes as humanity evolved. What began as the survival of a species through reproduction, eventually transformed into the early concept of marriage 4000 years ago⁵. Marriage in the olden days was vastly different to the concept of marriage that is much more popular in modern times. 4000 years ago, marriage was based on strategic alliances of Kingdoms. In both the Anglo-Saxon and Indian societies, marriage was viewed as a tool to establish political and commercial relationships between two kingdoms, or two nations. Consent from the woman to establish such an institution was largely absent from the equation. The presence of the bride and groom themselves was not particularly of importance, for the families were the ones who arranged the entire deal.

However, the meaning and understanding of marriage as an institution has vastly changed over the years. The changes in marriages happening in orthodox, patriarchal times to now, in a more egalitarian society, can be understood through a few key differences, such as that now, the consent from the woman is given more importance, and marriage is understood as the bond that is primarily between two individuals, and secondarily, between their families. But perhaps the most major of changes that has happened in marriage as an institution, is that increasingly, especially in India, children themselves are finding partners to marry, as opposed to parents looking for someone suitable for their child to marry. Live-in relationships and dating have taken a major step forward, and even though arranged marriages continue to happen in rural towns and villages, the urban landscape of India is seeing a shift towards love marriages, and marriages that happen subsequently after the partners have already familiarized themselves with each other for months, or even years.

This new shift towards an emphasis on dating has led to the invention of dating applications. The origins, or the idea behind dating apps can be traced back to early postages of profiles in the newspaper⁶, to the onslaught of matchmaking websites with the rise of the internet. The launch of Match.com in 1995 shifted matchmaking to the web, followed by sites like

⁵ Simran Sabharwal, *A jurisprudential understanding behind the evolution of marriage as an institution*, iPleaders (2019), <https://blog.ipleaders.in/jurisprudential-understanding-behind-evolution-marriage-institution/> (last visited July 14, 2026).

⁶ Susie Lee, *The History of Online Dating From 1695 to Now*, HuffPost 22 (2016), https://www.huffpost.com/entry/timeline-online-dating-fr_b_9228040 (last visited July 14, 2026).

eHarmony in 2000 and OkCupid in 2004, which used questionnaires to calculate compatibility⁷. Grindr, a popular dating application, launched in 2009 following the popularity of matchmaking websites. It utilized smartphone GPS technology to show users potential matches in their immediate physical proximity, which was a new feat at the time. The rise of Tinder in 2012 popularized the “swipe right/left” mechanic. It streamlined dating, at the time by integrating Facebook data to verify identities and make browsing rapid, visual and casual. What has followed since has been an onslaught of other dating apps, such as Bumble, Hinge, to the very latest ones like Schmooze, where you get matched with a potential partner based on preferences on social media popular trends and memes.

However, these dating applications were not without their negative side effects.

MAJOR USER SAFETY ISSUES AND LAWS DEALING WITH THEM

Online dating applications have become a major medium for initiating interpersonal and romantic relationships; however, their widespread use has also produced a distinct set of user safety concerns. The existing literature broadly groups these risks into privacy and security threats, deceptive or antisocial conduct, psychological harms, and physical or sexual safety concerns. In the Indian legal context, these concerns do not exist in isolation; rather, they intersect with the IT Act, 2000, the IT Rules, 2021, the DPDP Act, 2023, the BNS, 2023, and where minors are involved, the POCSO, 2012.

The first main concern is the compromise of user privacy. Dating platforms often involve the disclosure of sensitive personal information, including photographs, location data, relationship preferences and intimate communication. This information may be exposed through weak platform safeguards, unauthorized data access, screenshot circulation, impersonation, or large-scale data breaches, thereby increasing the risk of surveillance, doxxing, and reputational harm. These concerns are directly engaged by the DPDP Act, 2023, which creates liabilities for lawful processing⁸, consent⁹, purpose limitation, data minimisation, security safeguards, breach intimation, and grievance redressal¹⁰. The Act also interconnects with the IT Act, 2000, particularly provisions dealing with identity theft¹¹,

⁷ Pratyusha Pal, *Emergence of online dating apps & its psychological impact*, 26 IJPS 8, 5 (2024), <https://www.psychologyjournal.net/archives/2024/vol6issue1/PartA/6-1-3-372.pdf> (last visited July 14, 2026).

⁸ Digital Personal Data Protection Act, No. 22 of 2023, §4, ch. II (India).

⁹ Digital Personal Data Protection Act, No. 22 of 2023, §6, ch. II (India).

¹⁰ Digital Personal Data Protection Act, No. 22 of 2023, §13, ch. II (India).

¹¹ Information Technology Act, 2000, § 66C (India).

cheating by personation using computer resources¹², violation of privacy¹³, and failure to protect data, while the IT Rules, 2021, reinforce due diligence and grievance-handling duties of the intermediary platform for unlawful or privacy-invasive material¹⁴.

The second major issue is deception, which includes catfishing, identity misrepresentation, and the use of fraudulent profiles. These practices undermine trust and create a range of harmful outcomes, like emotional manipulation and scam-based exploitation. In particular, romance scams often rely on “love-bombing” before requests for money, gifts, or confidential information start pouring in. Such conduct may attract criminal consequences under the BNS, 2023, including offences involving cheating¹⁵, cheating by personation¹⁶, criminal intimidation¹⁷, extortion¹⁸, stalking¹⁹, voyeurism²⁰, and sexual harassment²¹, depending on the particular facts of the case. Where fake profiles are used to facilitate online fraud or impersonation, the intermediary’s due diligence obligations under the IT Rules, 2021²², also become relevant, especially if the platform fails to act on complaints or lacks reasonable reporting and takedown systems.

As discussed earlier, harassment and abuse also constitute a substantial category of risk. Users frequently report unwanted sexual messaging, coercive behaviour, stalking, repeated contact after rejection, and other forms of annoyances. Existing literature characterizes these behaviours as part of a broader pattern of antisocial conduct enabled by anonymity, easy access, and low-cost account creation associated with digital dating environments. In legal terms, these acts may fall within the BNS, 2023, particularly the provisions relating to stalking, sexual harassment, criminal intimidation, and other threatening or privacy-violating conduct, on a case-to-case basis. If the abuse occurs online, the IT Act, 2000 and the IT Rules, 2021, stay relevant because they provide a framework for intermediary responsibility, complaint handling, and penalties for misconducts.

Physical safety risks emerge most clearly when online interactions transition into offline meetings, such as dates. After talking only through an electronic medium, when the

¹² Information Technology Act, 2000, § 66D (India).

¹³ Information Technology Act, 2000, §§ 66E, 72, 72A (India).

¹⁴ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (India).

¹⁵ Bharatiya Nyaya Sanhita, 2023, § 318 (Cheating) (India).

¹⁶ Bharatiya Nyaya Sanhita, 2023, § 319 (Cheating by Personation) (India).

¹⁷ Bharatiya Nyaya Sanhita, 2023, § 351 (Criminal Intimidation) (India).

¹⁸ Bharatiya Nyaya Sanhita, 2023, § 308 (Extortion) (India).

¹⁹ Bharatiya Nyaya Sanhita, 2023, § 78 (Stalking) (India).

²⁰ Bharatiya Nyaya Sanhita, 2023, § 77 (Voyeurism) (India).

²¹ Bharatiya Nyaya Sanhita, 2023, § 75 (Sexual Harassment) (India).

²² Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r. 3 (India).

conversations go to an offline mode, it can expose catfishers and people who lied in their dating-app profiles. These concerns are particularly pronounced when users share their location or personal routines too early in the interaction. Where conduct escalates into sexual violence, kidnapping²³, wrongful confinement²⁴, assault²⁵, or criminal force²⁶, the BNS, 2023, again, provides the principal criminal law framework for prosecution. If a child is involved, the POCSO, 2012 takes the wheel, since it applies to sexual offences against persons below eighteen years of age and establishes child-friendly mechanisms for reporting, investigation, and trial²⁷.

In addition to these direct risks, dating app use has also been associated with adverse psychological outcomes. Repeated rejection, ghosting, objectification, and appearance-based evaluation may contribute to stress, reduced self-esteem, body image concerns or body dysmorphia, and emotional fatigue. Accordingly, the risks of dating apps should not be understood solely in terms of physical security, but also as issues affecting mental, relational and sexual well-being. From a regulatory perspective, these harms strengthen the case for platform-level safeguards under the IT Rules, 2021, and the DPDP Act, 2023, both of which reflect a broader move toward accountability in digital environments.

RELEVANT CASE LAWS

One common risk of a dating application is the very real possibility of a catfish, or people turning out to be the complete opposite of how they described themselves online. In India, the case of *Amardeep Singh v. State (GNCT of Delhi) & Anr.* stands out as involving allegations of coercion where the parties met on a dating application. According to the facts of the case as provided by the Delhi High Court, the parties met on the dating application “Bumble”. The prosecution’s version was that the petitioner and the complainant met through the dating application, developed a relationship, and later, the complainant alleged sexual exploitation and related offences; the defence argued that the relationship was consensual and there had been no promise to marry. The court’s discussion in this case focused on the nature of the relationship as the parties met on a dating application, the issue of consent, and whether the

²³ Bharatiya Nyaya Sanhita, 2023, § 137 (Kidnapping) (India).

²⁴ Bharatiya Nyaya Sanhita, 2023, § 127 (Wrongful Confinement) (India).

²⁵ Bharatiya Nyaya Sanhita, 2023, § 130 (Assault) (India).

²⁶ Bharatiya Nyaya Sanhita, 2023, § 129 (Criminal Force) (India).

²⁷ Protection of Children from Sexual Offences Act, 2012, §§ 24–25, 27 (India).

allegations justified continued custody, ultimately treating it as a matter fit for bail consideration rather than a straightforward case of coercion²⁸.

While there are not many case laws in India that view dating applications and user safety from a platform-liability angle, Indian courts have discussed the intermediary protection that such dating applications owe the users, especially under the IT Act. It also discusses whether platform operators can be prosecuted for users' conduct, especially in the Shaadi.com/Anupam Mittal litigation²⁹. The facts of the abovementioned litigation are that a complainant alleged harassment, cheating and extortion after using Shaadi.com, and the police initially tried to make Anupam Mittal personally liable as the founder/CEO. The complainant said that he created a profile on Shaadi.com, encountered obscene and blackmailing conduct from another user and then complained to the platform and to Mittal directly; when the issue was not resolved, the complainant filed the FIR. The FIR named Mittal and invoked offences such as cheating, extortion, criminal intimidation, conspiracy, and obscenity, but the Allahabad High Court later held that no active personal role by Mittal was shown and quashed the proceedings against him.

Internationally, the Competition and Markets Authority of the UK investigated online dating services for potentially unfair contract terms, misleading claims, and privacy/data issues, which directly bears on user safety and platform transparency³⁰. The case revolved around the Venntro Media Group, and looked at possible consumer-law breaches as well, focusing on how the service was advertised, how personal data was used, and whether subscription and cancellation terms were unfair or misleading. The case ended with undertakings from Venntro Media Group Limited to make its dating-service terms clearer, improve privacy, disclosures, avoid misleading claims about members and services, add clearer subscription and cancellation warnings, and provide some refunds and cancellation rights, while the CMA also warned other dating providers after its wider review. In the European Union, in the case of Facebook v. Bundeskartellamt³¹, a bigger safety issue is discussed; although it is not a dating-application case, it is important for platforms that combine services like social

²⁸ Amardeep Singh v. State (Govt. of NCT of Delhi) & Anr., Bail Application No. 72 of 2025, decided on 12 Feb. 2025 (Del. H.C.).

²⁹ Anupam Mittal v. State of Telangana & Ors., SLP (Crl.) No. 9356 of 2025; Vignesh v. State of Telangana & Ors., SLP (Crl.) No. 9362 of 2025 (S.C. Feb. 3, 2026).

³⁰ Competition & Markets Auth., Online Dating Services (Oct. 31, 2017), <https://www.gov.uk/cma-cases/online-dating-services> (last visited, 14th July, 2026.)

³¹ Case C-252/21, Meta Platforms Inc. v. Bundeskartellamt, ECLI:EU:C:2023:537 (July 4, 2023) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62021CJ0252> (last visited, 14th July, 2026.)

networking and dating features to tighten safety protocols because it addresses data protection and the use of user data across services.

Since dating applications and their widespread usage is still a relatively newer concept for Indians and India, there are no major case laws available in this regard. But many users have spoken out about their negative experiences using dating applications on social media, invoking a need for amendments and changes to be brought about in this regard.

AMENDMENTS IN USER SAFETY FOR ONLINE DATING APPS

As per everything discussed in the paper about dating applications and user safety, India could lawfully tighten online dating app safety through a mix of targeted amendments and perhaps a new standalone statute. The strongest existing legal base already comes from the IT Act, the IT Rules, the DPDP Act, the BNS, and POCSO, so a new law would mainly formalize platform-specific duties rather than start from zero. The government has already described the existing framework as covering identity theft, impersonation, privacy violations, obscene content, intermediary due diligence, child data protection, and cyber-enabled offences. That means Indian law already has tools to punish scams, harassment, sexual extortion, fake profiles, and unlawful content on dating apps. The gap is not total absence of law; it is the absence of rules tailored to dating platforms' risks.

A practical reform package could amend the IT Rules to treat dating applications as a distinct class of intermediaries with extra safety duties. The law could require mandatory but privacy-preserving age verification, stronger user reporting tools, faster takedown timelines for impersonation and non-consensual intimate content, and escrow-like preservation of evidence for police requests. It could also require clear consent screens, easy blocking, location-sharing controls, and special safeguards for users who disclose sensitive personal data. A dating app safety code could require verified profiles, periodic re-verification, visible risk warnings, and anti-catfishing measures for repeat offenders. Platforms could be asked to maintain dedicated grievance officers, emergency response channels for stalking or blackmail, and mandatory cooperation with law enforcement in serious cases. For children, the rules should go further and prohibit onboarding of minors, because the DPDP and POCO framework already shows the legal system treats child safety as a separate, stricter category.

As for a new, standalone law, the Parliament could pass a new law focused purely on online dating applications and user safety, and that would likely be cleaner than stretching general

intermediary law too far. A 2026 Parliamentary proposal already points in that direction by recommending mandatory KYC-based verification across dating platforms to curb fake profiles, impersonation, and anonymous harassment³². A dedicated statute could also define dating-service obligations, penalties, audit duties, identity verification limits, and victim support mechanisms in one place. A possible ‘Online Dating Platforms Safety Act’ could contain these elements:

1. Mandatory age assurance and prohibition on minors.
2. Verified-user options, with periodic re-verification for high-risk accounts.
3. Strict rules on impersonation, stalking, non-consensual sharing, and extortion.
4. Fast takedown and preservation-of-evidence duties.
5. Transparency reports, safety audits, and platform liability for repeated non-compliance.
6. Data-minimization rules under the DPDP framework, with bans on unnecessary sensitive-data collection.

The main legal debate would be between safety and privacy. Mandatory KYC can reduce fake profiles, but it also increases data-security risk and may chill legitimate use, so a proportionality-based design would be important. A better model may be tiered verification: real-name verification for high-risk features, while still allowing limited pseudonym use for ordinary browsing, provided the platform can trace serious abuse when lawfully required.

CONCLUSION

Online dating applications have transformed the manner in which individuals form relationships, communicate, and negotiate intimacy, but they have also introduced a distinct and escalating set of legal and safety concerns. As this paper has shown, the risks associated with such platforms extend far beyond mere inconvenience or social discomfort; they include privacy violations, impersonation, fraud, stalking, coercion, image-based abuse, sexual harassment, and, in extreme cases, physical and sexual violence. These harms are intensified by the very design of dating platforms, which often rely on anonymity, rapid matching, behavioural profiling, and the disclosure of sensitive personal data.

³² T. Vrinda, *Love in the Time of KYC: House Panel Wants KYC Made Mandatory for Social Media, Dating, Gaming Apps*, THEPRINT (23 March, 2026 05:10 pm IST), <https://theprint.in/india/governance/love-in-the-time-of-kyc-house-panel-wants-kyc-made-mandatory-for-social-media-dating-gaming-apps/2886501/>. (last visited, 14th July, 2026)

The existing Indian legal framework does provide an important, though fragmented, basis for response. The Information Technology Act, 2000, the IT Rules, 2021, the Digital Personal Data Protection Act, 2023, the Bharatiya Nyaya Sanhita, 2023, and POCSO Act together create a broad matrix of protections that can address different dimensions of online dating-related harm. Yet, as this paper has demonstrated, these laws were not drafted with dating applications specifically in mind. Their application is, therefore, often indirect, reactive, and uneven, leaving important gaps in platform accountability, preventive safety design, and user redress.

What emerges, then, is not a total absence of law, but a lack of a tailored and coherent regulatory framework. Dating applications occupy a uniquely sensitive digital space where issues of consent, identity, trust, and vulnerability intersect. A more effective legal approach must therefore balance autonomy with safety, and innovation with responsibility. This may require clearer intermediary duties, stronger verification safeguards, faster grievance redressal, and better protection for minors and other vulnerable users.

Ultimately, online dating cannot be treated as a purely private or technological matter. It is also a question of dignity, security, and legal accountability. As digital intimacy becomes more embedded in everyday life, the law must evolve to ensure that the freedom of connection does not come at the cost of personal safety.