
GHOSTED BY THE LAW: ACCOUNTABILITY GAPS IN INDIA'S ONLINE DATING INDUSTRY - A DOCTRINAL AND COMPARATIVE STUDY OF PLATFORM LIABILITY, DATA PROTECTION AND CRIMINAL REMEDIES IN THE INDIAN ONLINE DATING INDUSTRY

Parth Singh & Hetansh Chandiramani, B.A. LL.B., Thakur Ramnarayan College of Law

ABSTRACT

Online dating is no longer rare in India. Dating apps and matrimonial websites are now used by a large and growing number of Indians to find a partner. However, the law has not kept pace with this shift. Dating platforms are not named in any Indian law. Instead, they are governed by four general sets of rules: the intermediary provisions of the Information Technology Act, 2000; the due diligence duties in the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021; the consent-based duties of the Digital Personal Data Protection Act, 2023; and consumer protection law. These rules were not made with romance fraud, catfishing, sextortion or matching algorithms in mind. The resulting accountability gap is examined in this paper. The term refers to the gap between the harm that can be caused through a dating platform and the liability that is actually placed on it. The laws that govern these platforms are traced. The criminal provisions that can be used by a victim after the harm are listed. The court-made rule of safe harbour, under which platforms are protected from liability for the acts of their users, is also studied. This framework is then tested against National Crime Records Bureau data, two Delhi police cases reported in the national press, and the rules followed in the United States and the United Kingdom. It is concluded that a dating app is treated in India like any other website that carries user content. But the product is different. It is built to bring strangers together in person on the basis of a profile that has never been checked. Three objections to reform are also answered. Five practical reforms are then proposed: a due diligence code for dating platforms, mandatory safety disclosures based on the Texas model, a dedicated grievance and compensation system, penalties linked to platform revenue and public legal awareness campaigns. Through these reforms, the gap can be closed without dating platforms being turned into surveillance systems.

Keywords: Online Dating, Intermediary Liability, Information Technology Act 2000, Digital Personal Data Protection Act 2023, Safe Harbour, Catfishing, Sextortion, Consumer Protection, Platform Accountability, Data Protection

I. Introduction

1.1 The Rise of the Digital Courtship Economy in India

Twenty years ago, meeting a partner through a screen was seen as strange and even suspicious in most Indian homes. That view has changed. Dating apps such as Tinder, Bumble and Hinge are now used alongside well-known matrimonial websites such as Shaadi.com and BharatMatrimony. These platforms are used for everything from casual dating to familyarranged marriage.¹

This growth has been driven by convenience. An introduction through family, work or friends is no longer needed. The introduction is made by an algorithm instead. It is based on a profile written by the user and photographs chosen by the user. But this convenience depends on one claim that is never checked: that the person on the other side of the screen is who the profile says they are. When that claim turns out to be false, the harm can range from wasted time and hurt feelings to financial fraud, sexual exploitation and, in some cases, violence.

The law has not kept up with this change. Some similar high-risk digital services are already controlled by special rules in India. For example, ride-hailing companies are required by the Motor Vehicle Aggregator Guidelines, 2025 to have their drivers checked, including through police verification, before the drivers are taken on.² No such rules have been made for online dating. A dating platform is treated by Indian law in the same way as a photo-sharing app or a discussion forum. It is simply called an “intermediary” under the Information Technology Act, 2000. Whether this general treatment is adequate for a product designed to move a relationship from the screen to a real meeting is the central question of this paper.

1.2 Statement of the Problem

The main problem studied in this paper is a mismatch between risk and regulation. Some of

¹ Bismah Malik, *Stupid Cupid: How Dating Apps in India Have Become Crime Epicentres*, Inc42 (Feb. 14, 2024).

² Ministry of Road Transport & Highways, Motor Vehicle Aggregator Guidelines, 2025 (July 2025) (India).

the most sensitive data a person can share is collected by dating platforms. This includes sexual orientation, relationship status, location and, more and more often, selfie images used for verification. Yet little assurance is given that the person receiving this data is genuine. Parts of this problem are covered indirectly by Indian law. Cheating, impersonation, extortion and image-based abuse are all treated as crimes. But these laws can be used by a victim only after the harm has been done. The introduction was designed by the platform, money was made from it by the platform, and the data needed to identify the wrongdoer is held only by the platform. Even so, almost no separate duty to prevent the harm is placed on the platform, and wide protection from liability is given to it once the harm has occurred.³

This is the accountability gap from which the title of this paper is taken. A user who is “ghosted” after being deceived, cheated or exploited often finds that little is offered by the law as well. Only a criminal complaint can be filed, and it is often filed against a person who cannot be traced, who uses a fake identity or who lives outside the area of the local police station.

1.3 Research Objectives

Five objectives are set for this paper. First, the laws that apply to online dating platforms in India are mapped. These include intermediary law, data protection law and consumer protection law. Second, the criminal provisions that can be used by a victim under the Bharatiya Nyaya Sanhita, 2023 and the Information Technology Act, 2000 are listed. Third, the court decisions on safe harbour and the right to privacy are traced. The amount of responsibility a platform bears for its users is shaped by these decisions. Fourth, the Indian position is compared with the models used in the United States and the United Kingdom, where direct duties are placed on dating and social platforms. Fifth, practical reforms are suggested through which the gap can be narrowed without user privacy being harmed.

1.4 Research Questions

Four questions are addressed in this paper. First, is any duty placed on a dating platform by Indian law that responds to the special risks of dating platforms, or are only the duties common to all intermediaries imposed? Second, as Section 79 of the Information Technology Act, 2000 is currently read by the courts, are dating platforms protected by its safe harbour from liability for harms that can be foreseen, such as catfishing and extortion? Third, is the way user data is

³ See Malik, *supra* note 1.

collected, kept and sold by dating platforms properly checked by the Digital Personal Data Protection Act, 2023? Fourth, which tools used in other countries could be adopted by India, such as disclosure duties, risk assessments and rewards for verification? And can they be adopted without users being forced to hand identity documents to private companies?

1.5 Scope and Limitations

Only platforms whose main purpose is to connect people for dating or marriage are covered in this paper. Both casual dating apps and matrimonial websites are included, because strangers are introduced by both on the basis of an unchecked profile. General social media platforms are not covered, except where features such as direct messaging and location sharing can be directly compared. The paper is based on a study of statutes and case law. This study is supported by National Crime Records Bureau data and by reports of specific incidents published in established national newspapers. No surveys or interviews were conducted. Only two countries, the United States and the United Kingdom, are covered in the comparative section. They were chosen because laws on platform safety and disclosure have been passed in both, and useful lessons for India can be drawn from them. The European Union's Digital Services Act is noted briefly in Part IX, but it is not used as a main model.

II. Research Methodology

The doctrinal method of legal research is used in this paper, and it is supported by a comparative and policy-based approach. The primary sources studied are the Information Technology Act, 2000 and its 2008 amendment; the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021; the Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025; the Bharatiya Nyaya Sanhita, 2023; the Consumer Protection Act, 2019 and the Consumer Protection (E-Commerce) Rules, 2020; and the judgments of the Delhi High Court and the Supreme Court of India by which the law on intermediary liability and privacy has been shaped.⁴

The secondary sources used are the National Crime Records Bureau reports on crime in India

⁴ Information Technology Act, No. 21 of 2000, India Code (2000); Information Technology (Amendment) Act, No. 10 of 2009, India Code (2009); Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E) (India); Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023); Digital Personal Data Protection Rules, 2025 (India); Bharatiya Nyaya Sanhita, No. 45 of 2023, India Code (2023); Consumer Protection Act, No. 35 of 2019, India Code (2019); Consumer Protection (E-Commerce) Rules, 2020, G.S.R. 462(E) (India).

for 2023 and 2024, the legislative record of the State of Texas, academic legal writing, a Human Rights Watch report and reports published in established newspapers and legal publications.⁵ Informal or unverified material has been deliberately left out. This includes social media comments, anonymous forum posts, commercial marketing content and unmoderated review websites. The standard of evidence required for a legal research paper is not met by any of these. Where a factual claim could not be traced to an authoritative source, it was removed.

A functional method is used in the comparative section. Foreign law is not copied as a whole. Instead, the specific technique used in each country is identified: a disclosure rule under Texas law and risk assessment duties under the United Kingdom's Online Safety Act, 2023. It is then asked whether a similar technique could be used within India's constitutional and administrative system.⁶

III. Literature Review

3.1 On Intermediary Liability and Safe Harbour

Any study of platform liability in India begins with Section 79 of the Information Technology Act, 2000. This section was rewritten by Parliament through the Information Technology (Amendment) Act, 2008.⁷ The change was made after a gap in the original law was exposed by the prosecution of the chief executive of Bazeem.com.⁸ Only narrow protection was given by the original section. Platform executives could be prosecuted for content that had not been created by them and could not practically have been checked by them. This was replaced by a conditional immunity in the amended section. A platform is not held liable for user content if it acts only as a passive carrier, if due diligence is observed and if unlawful content is removed once actual knowledge of it is gained. In *Shreya Singhal v. Union of India*, "actual knowledge" was read by the Supreme Court to mean a court order or a notice from the proper government agency.⁹ It was reasoned by the Court that intermediaries cannot be expected to decide for themselves whether content is lawful. Through this ruling, the situations in which safe harbour

⁵ Nat'l Crime Records Bureau, Ministry of Home Affs., *Crime in India 2023* (2025); Nat'l Crime Records Bureau, Ministry of Home Affs., *Crime in India 2024* (2026).

⁶ Tex. Bus. & Com. Code Ann. §§ 106.001 et seq. (added by Acts 2011, 82d Leg., R.S., ch. 27 (S.B. 488), § 1, eff. Sept. 1, 2011); Online Safety Act 2023, c. 50 (UK).

⁷ Information Technology (Amendment) Act, No. 10 of 2009, India Code (2009) (substituting Section 79 of the Information Technology Act, 2000).

⁸ *Avnish Bajaj v. State (NCT of Delhi)*, 116 (2005) DLT 427 (Del.) (India).

⁹ *Shreya Singhal v. Union of India*, (2015) 5 SCC 1 (India).

is lost by a platform were narrowed even further. The wider constitutional risk of this area of law has been examined in academic writing. It has been argued by Chinmayi Arun that platforms act as gatekeepers of information, and that liability placed on them can be used to restrict speech in ways that are hard for the public to see.¹⁰ This concern helps to explain why the courts have been slow to widen the duties of intermediaries.

3.2 On Platform-Enabled Fraud in the Indian Dating Market

In business reporting, the Indian dating industry is described as under-regulated compared to the harm caused through it. In a 2024 Inc42 feature, it is noted that dating apps are treated as intermediaries, so the same grievance officer and content duties must be met by them as by any other platform. A human rights activist quoted in the feature claims that these rules have been largely ignored by dating apps, unlike large social media companies. It is also claimed by her that the penalties are too small for the behaviour of these apps to be changed.¹¹ These are the views of one activist and have not been tested by any official study. The wider picture is supported by newspaper reports of police investigations. These reports show dating and matrimonial platforms being used for sextortion and organised extortion in Delhi.¹² Two such cases are examined in Part VIII.

3.3 On Data Protection and Dating Platforms

In legal commentary published after the Digital Personal Data Protection Rules, 2025 were notified, dating apps such as Bumble, Hinge and Tinder are treated as “data fiduciaries” under the Digital Personal Data Protection Act, 2023. Particular concern is raised in that commentary about data that is kept by apps even after a profile is deleted. This includes device identifiers, location signals and data already passed to advertisers. The right to erasure under Section 12 and the purpose limitation under Section 6 are seen by its authors as a direct answer to this practice.¹³ Before 2023, such data was protected mainly by Section 43A of the Information Technology Act, 2000 and the rules made under it, which are narrower in scope. In United

¹⁰ Chinmayi Arun, *Gatekeeper Liability and Article 19(1)(a) of the Constitution of India* (Ctr. for Commc’n Governance, Nat’l L. Univ. Delhi, Working Paper, May 20, 2015).

¹¹ Malik, *supra* note 1.

¹² *Delhi Man Impersonates as Model from US, Blackmails Over 700 Women on Bumble, Snapchat with Private Photos*, The Tribune (Jan. 4, 2025); Samad Hoque, *App Date Turns Costly for Civil Services Aspirant*, The Tribune (June 28, 2024).

¹³ Nandita Goyal & Archit Vyas, *Ghosts in the Machine: Dating Apps and the DPDP Act*, Bar & Bench (Dec. 11, 2025).

States commentary, where no similar federal law exists, research by the Mozilla Foundation is cited. According to that research, eight in ten dating apps studied may pass users' personal data to others or sell it, and the same apps give no firm promise that data will be deleted when a user asks.¹⁴ It is argued in this paper that a similar pattern may continue in India unless the Act is enforced actively by the Data Protection Board of India, rather than only when complaints are filed.¹⁵

3.4 On Comparative Safety Regulation

The legislative record in Texas shows that the special safety risk of dating platforms was recognised early, because strangers are introduced through them. Texas lawmakers were concerned that background checks on users were being run by only a small share of the sites used by the public.¹⁶ A modest duty was introduced in response. Users must be told by platforms whether or not background checks are run, but the checks themselves are not required. In the United Kingdom, "user-to-user services" are regulated by the Online Safety Act, 2023, and this definition is wide enough to include dating apps. These services are required to assess the risk of illegal content and, where they are likely to be used by children, the risk of harm to children.¹⁷ These duties are enforced by the communications regulator, Ofcom. A shift from safe harbour protection towards an active duty of care is marked by this Act.

3.5 On Trust, Design and User Safety

The safety of dating platforms has also been studied in academic legal writing. In a study of gay and bisexual men who use location-based dating apps, it was found by Ari Ezra Waldman that these users are victims of the non-consensual sharing of intimate images more often than the general population.¹⁸ In later work, it is argued by Waldman that an online space in which personal information is shared can be made safe only when the pressure to share is balanced by trust. That trust must be built into the design of the platform and supported by law.¹⁹ This view supports the argument made in this paper. The safety of users depends on how a dating

¹⁴ Kiara J. Patiño Navarro, *Identity & Criminal Check Verification: Potential Solution to Bridging the Safety Gap in Dating Apps*, Cal. Laws. Ass'n (May 30, 2025) (citing Mozilla Foundation research).

¹⁵ Cf. Goyal & Vyas, *supra* note 13.

¹⁶ House Comm. on Tech., Bill Analysis, Tex. C.S.H.B. 1052, 82d Leg., R.S. (2011) (House companion to S.B. 488).

¹⁷ Online Safety Act 2023, c. 50, §§ 3, 9, 11 (UK).

¹⁸ Ari Ezra Waldman, *Law, Privacy, and Online Dating: "Revenge Porn" in Gay Online Communities*, 44 Law & Soc. Inquiry 987 (2019).

¹⁹ Ari Ezra Waldman, *Safe Social Spaces*, 96 Wash. U. L. Rev. 1537 (2019).

platform is designed, and not only on how individual users behave.

When this literature is read together, the central argument of this paper is supported. The regulation of dating platforms in India has not kept up with the technology. Workable models for closing that gap are offered by similar jurisdictions.

IV. Dating Platforms Under Indian Law: The Existing Regulatory Map

4.1 Classification as Intermediaries under the IT Act, 2000

“Dating platform” and “matrimonial platform” are not recognised as separate legal categories by Indian law. Instead, every dating app is classed as an “intermediary” under Section 2(1)(w) of the Information Technology Act, 2000, because messages and profiles are received, stored or sent by the app on behalf of its users.²⁰ Through this classification, the platform is brought within the safe harbour under Section 79. Under that section, an intermediary is exempted from liability for third-party content if certain conditions are met. The sending of the content must not be started by the intermediary, the receiver must not be selected by it and the content must not be changed by it. The due diligence set by the Central Government must also be observed. In practice, a dating platform is therefore not held legally responsible by default for a fake, false or abusive profile created by one of its users. Responsibility is placed by the law on the user who created the profile. It is not placed on the platform by which the profile was hosted, ranked and shown to a possible match.

4.2 The IT Rules, 2021 and Due Diligence Obligations

Conditions are attached to the Section 79 safe harbour by the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. A privacy policy and terms of service must be published by every intermediary, and users must be told which content is prohibited. A Grievance Officer must also be appointed. User complaints must be acknowledged by this officer within twenty-four hours and resolved within fifteen days.²¹ A threshold of fifty lakh registered users in India has been set by the Central Government. Platforms above this threshold are treated as “significant social media intermediaries”. A Chief Compliance Officer, a Resident Grievance Officer and a Nodal Contact Person for coordination

²⁰ Information Technology Act, No. 21 of 2000, India Code (2000), §§ 2(1)(w), 79.

²¹ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E), rr. 3(1), 3(2)(a) (India) [hereinafter IT Rules].

with law enforcement must also be appointed by them. Monthly compliance reports must be published as well.²²

A faster process is also created by the Rules for content that shows nudity or sexual acts, or through which a person is impersonated, including by morphed images. This kind of imagebased abuse is directly relevant to dating platforms. Once a complaint is made by the affected person, or by someone on their behalf, such content must be removed by the platform within twenty-four hours.²³ However, these duties begin only after the content has been posted and, in most cases, after it has already been seen by others. Under none of them is a dating platform required to verify a user's identity, age or marital status before a profile is created and other users are contacted. Yet this is exactly the point at which catfishing and matrimonial fraud begin.

4.3 The Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 is India's first complete data protection law. When it is read with the Digital Personal Data Protection Rules, 2025, dating platforms are treated as "data fiduciaries".²⁴ Personal data may be processed by a platform only with free, specific, informed and revocable consent, or for one of the limited "certain legitimate uses" listed in Section 7.²⁵ ²⁶Reasonable security safeguards must be adopted, and any breach must be reported to the Data Protection Board of India and to the affected users. Personal data must also be erased once it is no longer needed for its purpose or once consent is withdrawn by the user. These duties are brought into force by the Rules in stages. The Rules were notified in November 2025. The Data Protection Board was set up at once, but the core duties of data fiduciaries, including notice and consent, security safeguards, breach reporting and the rights of users, come into force only eighteen months later, in May 2027. Until then, sensitive user data held by dating platforms is governed mainly by Section 43A of the Information Technology Act, 2000 and the rules made under it in 2011. Under those rules, sexual orientation is treated as "sensitive personal data", and reasonable security practices must be followed by any company that handles it. Where such data is misused because those practices

²² *Id.* r. 4(1); Ministry of Elec. & Info. Tech., Notification S.O. 942(E) (Feb. 25, 2021) (India).

²³ IT Rules, *supra* note 21, r. 3(2)(b).

²⁴ Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023), § 2(i).

²⁵ *Id.* §§ 6–7.

²⁶ *Id.* § 8(5)–(7).

were not followed, compensation may be claimed by the affected user under Section 43A.²⁷

On paper, heavy penalties are set by the Act, and they can be imposed once its core duties take effect. A penalty of up to two hundred and fifty crore rupees can be imposed for a failure to keep reasonable security safeguards. A penalty of up to two hundred crore rupees can be imposed for a failure to report a breach.²⁸ This matters for dating platforms, because sexual orientation, religion and location are regularly revealed in profiles. If this data is misused, a user can be exposed to serious physical and social risk. The risk is greater in a country where consensual same-sex relations were decriminalised by the Supreme Court only in 2018.²⁹ Yet the Act is built on a notice-and-consent model. The risk that consent is given to share data with a person whose stated identity is false is not addressed by this model.

4.4 Consumer Protection Law and E-Commerce Rules

Dating platforms that charge for premium features are also covered by consumer protection law. Misleading advertisements and unfair trade practices are prohibited by the Consumer Protection Act, 2019. Under the Consumer Protection (E-Commerce) Rules, 2020, e-commerce entities are required to give accurate information about the services offered by them. Paid dating platforms arguably fall within this group, although this has not yet been settled by any court or authority.³⁰ This framework can be used for a narrow type of complaint, such as a case where a user is misled about what a paid subscription offers. It was not designed for romance fraud, catfishing or physical safety. No more protection against a fraudulent match is given to a paying user than to a free user.

4.5 The Regulatory Vacuum: No Sector-Specific Statute

When this framework is seen as a whole, a structural feature rather than an oversight is revealed. A dating platform is regulated in India in exactly the same way as a discussion forum, a photo-sharing app or an online marketplace. No duty is imposed by Indian law that responds to what makes a dating platform different. The whole design of such a platform is aimed at

²⁷ Digital Personal Data Protection Rules, 2025, r. 1 (India); Information Technology Act, *supra* note 20, § 43A; Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, G.S.R. 313(E), r. 3 (India).

²⁸ Digital Personal Data Protection Act, *supra* note 24, § 33, sch.

²⁹ *Navtej Singh Johar v. Union of India*, (2018) 10 SCC 1 (India).

³⁰ Consumer Protection Act, No. 35 of 2019, India Code (2019), §§ 2(28), 2(47); Consumer Protection (E-Commerce) Rules, 2020, G.S.R. 462(E), r. 4 (India).

turning an online introduction into a face-to-face meeting between two strangers. A contrast is offered by other high-risk digital sectors. As noted in Part I, ride-hailing companies are required to verify their drivers, including through police verification, as a condition of their licence.³¹ No similar safety rules have been made for dating platforms, even though two strangers are brought into physical contact by them too.

V. Criminal Law and the Digital Dating Encounter

Once harm has been done, the general criminal law must be relied on by a victim of fraud, harassment or exploitation through a dating platform. No offence specific to online dating has been created by any Indian law. The provisions that are used most often are listed in this Part.

5.1 Catfishing and Cheating by Personation

“Catfishing” means that a false online identity is created to deceive another person, usually so that money, personal information or emotional investment can be obtained. Catfishing is not named as an offence in Indian law, but its elements are well covered by existing provisions. Cheating is punished under Section 318 of the Bharatiya Nyaya Sanhita, 2023. This section corresponds to Section 420 of the former Indian Penal Code, 1860. Where the victim is led by the deception to hand over property or a valuable security, imprisonment of up to seven years and a fine are prescribed by Section 318(4). Cheating by personation is punished separately under Section 319. This covers cases where a person pretends to be someone else, whether real or imaginary, in order to deceive. This section corresponds to Section 419 of the former Code, and imprisonment of up to five years, a fine or both can be imposed under it.³²

Where a computer resource is used, for example when a fake dating profile is created, Section 66D of the Information Technology Act, 2000 also applies. Under this section, cheating by personation using a computer resource is punished with imprisonment of up to three years and a fine of up to one lakh rupees. Under Section 66C, the fraudulent or dishonest use of another person’s “unique identification feature” is punished separately. It has not yet been settled by the courts whether photographs taken from an unconnected person fall within this phrase. The provision is still relevant where another person’s identity details are used by a catfisher to build

³¹ Motor Vehicle Aggregator Guidelines, *supra* note 2.

³² Bharatiya Nyaya Sanhita, No. 45 of 2023, India Code (2023), §§ 318(4), 319(2).

a false profile.³³

5.2 Sextortion, Voyeurism and Image-Based Abuse

A common pattern begins when trust is built by an offender through a dating platform and intimate photographs or videos are obtained. A threat is then made that these will be published unless money is paid. This practice is commonly called “sextortion”. Sextortion is not treated as a separate offence in Indian law, but several provisions are engaged by the conduct at once. Under the Bharatiya Nyaya Sanhita, 2023, a threat to publish intimate images in order to obtain money or anything of value is treated as extortion under Section 308. When an image of a woman engaged in a private act is captured or shared without her consent, voyeurism is committed under Section 77. When sexual favours are demanded from a woman, sexual harassment is committed under Section 75.³⁴ Under the Information Technology Act, 2000, the capture, publication or sending of an image of a person’s private area without consent is punished by Section 66E. The publication or sending of obscene and sexually explicit material is punished by Sections 67 and 67A respectively.³⁵

Where the victim is a child, the Protection of Children from Sexual Offences Act, 2012 is applied in addition to these provisions.³⁶ Dating platforms are expected to keep children out through minimum-age rules in their terms of service. Once the core duties of the Digital Personal Data Protection Act, 2023 take effect in May 2027, verifiable parental consent will also be required before a child’s data is processed by a data fiduciary.³⁷ But no law specifically requires the age of every user to be checked by a dating platform at sign-up so that children are kept out.

5.3 Extortion Through Manufactured Intimacy

A different pattern is seen when dating platforms are used by organised groups to lure a user to a particular place, usually a café or restaurant, rather than to cheat a match directly. An inflated bill is then given to the user by staff at the venue, and payment is forced through threats, confinement or intimidation. Extortion under Section 308 and criminal intimidation

³³ Information Technology Act, *supra* note 20, §§ 66C, 66D.

³⁴ Bharatiya Nyaya Sanhita, *supra* note 32, §§ 75, 77, 308.

³⁵ Information Technology Act, *supra* note 20, §§ 66E, 67, 67A.

³⁶ Protection of Children from Sexual Offences Act, No. 32 of 2012, India Code (2012).

³⁷ Digital Personal Data Protection Act, *supra* note 24, § 9(1).

under Section 351 of the Bharatiya Nyaya Sanhita, 2023 are engaged by this conduct. Where the scheme is coordinated by several people, the offence of criminal conspiracy under Section 61 also applies.³⁸ What separates this pattern from ordinary extortion is the role played by the platform. The platform is used by the offenders to find the victim, learn about them and bring them to the place of the offence. Yet no separate legal scrutiny is faced by the platform for that role.³⁹

5.4 Matrimonial Cyber Fraud

A related but different risk is presented by matrimonial platforms. Their stated purpose is marriage, and because of this, more trust is created than on a casual dating app. Fraud that is started on a matrimonial website can be moved to WhatsApp or another messaging app, where the relationship is deepened by the offender before money is asked for. The same provisions on cheating, personation and extortion are applied. Matrimonial websites are also used in organised schemes. In the Delhi café case discussed in Part VIII, one of the accused was arrested by the police while she was with a man she had met through a matrimonial website.⁴⁰ The same Section 79 safe harbour is enjoyed by matrimonial platforms as by casual dating apps. Under the present law, a user's fraud is not treated as conduct "aided" by the platform merely because the fraud was made possible by the platform's design.⁴¹

VI. Judicial Developments Shaping Platform Accountability

No case directly involving a dating platform has yet been decided by an Indian court. The law on platform liability that is followed today was developed in a dispute over an online auction site and in a constitutional challenge to limits on online speech. That law is still fully applied to dating platforms, because none of it depends on the type of content or service involved.

6.1 The Bazee.com Litigation and the Birth of Safe Harbour

The foundational case is *Avnish Bajaj v. State (NCT of Delhi)*. It arose in 2004 when an obscene video clip was sold through the online auction site Bazee.com.⁴² It was held by the Delhi High Court that the site's managing director could not be made liable under the Indian Penal Code,

³⁸ Bharatiya Nyaya Sanhita, *supra* note 32, §§ 61, 308, 351.

³⁹ See Hoque, *supra* note 12.

⁴⁰ Hoque, *supra* note 12.

⁴¹ Information Technology Act, *supra* note 20, § 79(3)(a).

⁴² *Avnish Bajaj*, *supra* note 8.

1860 merely because an offence had been committed on the site. His personal involvement had not been shown by the prosecution. However, the case was allowed by the Court to go ahead under Section 67 read with Section 85 of the Information Technology Act, 2000. It was reasoned that a duty of due diligence was owed by the platform, including where content had slipped past its own filters. In 2012, the proceedings against Bajaj were quashed by the Supreme Court. It was held that a director cannot be prosecuted under Section 85 unless the company itself is also made an accused.⁴³ Later, in *Sharat Babu Digumarti v. Government (NCT of Delhi)*, the case against another Bazeem.com manager was also quashed by the Supreme Court. It was held that where the conduct is specifically covered by the Information Technology Act, a charge under the general provisions of the Indian Penal Code cannot be added for the same conduct.⁴⁴

The legislative response to the Bazeem.com case was the 2008 amendment to Section 79.⁴⁵ The original narrow immunity was replaced by the present conditional safe harbour. An intermediary is not held liable for third-party content if it acts only as a passive carrier and unlawful content is removed once actual knowledge of it is gained. After *Shreya Singhal*, actual knowledge is understood to mean a court order or a government notice. This amendment is the most important piece of legislative history for understanding why so little legal risk is faced by dating platforms today for fake or dangerous profiles. A stricter standard might have been produced by this case. Instead, a more protective standard was produced. Parliament was moved by a fair concern that every piece of user content could not reasonably be checked by platforms in advance.

6.2 Shreya Singhal and the Narrowing of Intermediary Exposure

In *Shreya Singhal v. Union of India*, a constitutional challenge to Section 66A of the Information Technology Act, 2000 was heard by the Supreme Court. Under that section, the sending of “offensive” messages through a communication device was made a crime. Section 66A was struck down by the Court as vague and disproportionate. Section 79(3)(b) was also read down. It was held that an intermediary is not required to decide for itself whether user content is unlawful. Its duty to act arises only when a court order or a notice from the proper

⁴³ *Aneeta Hada v. Godfather Travels & Tours (P) Ltd.*, (2012) 5 SCC 661 (India).

⁴⁴ *Sharat Babu Digumarti v. Government (NCT of Delhi)*, (2017) 2 SCC 18 (India).

⁴⁵ Information Technology (Amendment) Act, *supra* note 7.

government agency is received.⁴⁶ For a dating platform, this means that no general legal duty is placed on it to check whether a profile is fake, whether the photographs belong to the user or whether the stated identity is genuine. Apart from the complaint-based duties in the 2021 Rules, that duty arises only once an order is received. A reactive system is the result. The platform's legal duty begins only after a fake profile has already been connected with a victim through the deception.

6.3 Sharat Babu Digumarti and the Limits of Employee Liability

A narrower but important lesson is also taught by *Sharat Babu Digumarti*. It was reasoned by the Court that where the conduct is specifically dealt with by the Information Technology Act, 2000, an individual cannot be exposed to wider liability under the general criminal law for the same conduct.⁴⁷ Through this, one route that might otherwise have pushed dating platforms towards better verification is closed: the threat of criminal liability for founders and compliance officers. Accountability is directed instead towards regulatory penalties under the 2021 Rules and the Digital Personal Data Protection Act, 2023. As is shown in Part VII, those penalties remain either small or untested against dating platforms.

6.4 Puttaswamy and the Constitutional Right to Digital Privacy

In *Justice K.S. Puttaswamy (Retd.) v. Union of India*, it was held in 2017 by a nine-judge bench of the Supreme Court that the right to privacy is part of the right to life and personal liberty under Article 21 of the Constitution. Any state action by which privacy is infringed must satisfy the tests of legality, necessity and proportionality.⁴⁸ The case arose from the challenge to the Aadhaar scheme, but the whole Digital Personal Data Protection Act, 2023 is built on its reasoning.

For dating platforms, *Puttaswamy* cuts both ways. On one hand, the case for stronger protection of a user's sexual orientation, relationship history and location is strengthened, because sexual orientation was expressly recognised in the judgment as a protected part of privacy. On the other hand, a warning is given against closing the accountability gap through intrusive identity or background checks. Any verification rule imposed by the state must itself pass the

⁴⁶ *Shreya Singhal*, *supra* note 9.

⁴⁷ *Sharat Babu Digumarti*, *supra* note 44.

⁴⁸ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).

proportionality test, and a blanket rule would struggle to do so. This concern is confirmed by the later Aadhaar judgment. In that judgment, Section 57 of the Aadhaar Act, 2016 was struck down by the Supreme Court. Under that section, private companies had been allowed to use Aadhaar authentication.⁴⁹

VII. Mapping the Accountability Gap

In this Part, the statutes in Part IV, the criminal provisions in Part V and the case law in Part VI are brought together. Five ways are identified in which Indian law falls short of the risk presented by dating platforms.

7.1 Safe Harbour as a Shield, Not a Standard

The Section 79 safe harbour, as it was later shaped by *Shreya Singhal* and the Bazeed.com cases, was designed by Parliament so that platforms would not be crushed by liability for content that cannot be checked by them. That reasoning suits a comment posted on a public forum. It suits a dating platform less well. User content is not merely hosted passively by a dating platform. It is actively selected. Specific profiles are ranked, filtered and shown to specific users through a matching algorithm that is designed and controlled by the platform. It is also claimed by a human rights activist quoted in industry reporting that the 2021 Rules have been largely ignored by dating apps, and that the penalties are too small for their behaviour to be changed.⁵⁰

7.2 The Absence of Mandatory Identity Verification

No Indian law requires a user's real identity, age or marital status to be verified by a dating platform before a profile is created and other users are contacted. Optional photo verification is offered by some platforms. A live selfie is taken by the user, and it is compared by the platform with the profile photographs. Only a resemblance between the person and their own photographs is confirmed by this. The person's legal name, age or criminal history is not confirmed. No Indian law requires criminal background checks to be run by a platform. Nor is a platform required by any law to tell users whether such checks are run.

⁴⁹ *Justice K.S. Puttaswamy (Retd.) v. Union of India (Aadhaar)*, (2019) 1 SCC 1 (India); Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, No. 18 of 2016, India Code (2016), § 57.

⁵⁰ See Malik, *supra* note 1.

7.3 Disproportion Between Statutory Penalty and Platform Revenue

Where penalties exist, they are rarely matched to the resources of the platforms at which they are aimed. No separate fine is set by the 2021 Rules for a failure to appoint a Grievance Officer or to resolve a complaint within fifteen days. The main consequence is that the Section 79 safe harbour is lost.⁵¹ That penalty is felt only if a specific piece of harmful content later becomes the subject of a court case. Larger penalties are available under the Digital Personal Data Protection Act, 2023, including up to two hundred and fifty crore rupees for a security failure. But these penalties depend on a breach being investigated and acted on by the Data Protection Board of India.⁵² At the time of writing, no enforcement record against dating platforms has been built by the Board. This is partly because most of the duties enforced by the Board do not take effect until May 2027.

7.4 Underreporting and the Data Mirage

A sharp rise in cybercrime in India is shown by National Crime Records Bureau data. The number of registered cases rose from 65,893 in 2022 to 86,420 in 2023, an increase of 31.2 per cent. It rose again to 1,01,928 in 2024, an increase of 17.9 per cent.⁵³ These figures are driven by fraud, which was recorded as the motive in 72.6 per cent of all cybercrime cases in 2024. By contrast, sexual exploitation was recorded as the motive in only 3,190 cases and extortion in only 2,536 cases across the whole country in 2024.⁵⁴ The harm addressed in this paper is probably understated by these figures. Only cases in which a First Information Report is registered by the police are counted by the Bureau, so harm that is never reported by victims cannot be captured. Victims of romance fraud and sextortion may also stay silent because of the shame attached to it. Moreover, no offence is tagged in Indian crime data as having been enabled by a dating platform. The true scale of the harm is therefore hidden in the national statistics. It is buried inside wider categories of cheating, extortion and sexual exploitation.

7.5 Data Monetisation Versus the Consent Fiction

The protection given by the Digital Personal Data Protection Act, 2023 is built around consent. Personal data may be processed by a data fiduciary where free, specific and informed consent

⁵¹ IT Rules, *supra* note 21, r. 7.

⁵² Digital Personal Data Protection Act, *supra* note 24, § 33, sch.

⁵³ *Crime in India 2023*, *supra* note 5; *Crime in India 2024*, *supra* note 5.

⁵⁴ *Crime in India 2024*, *supra* note 5.

is given by the data principal for a clearly stated purpose.⁵⁵ A right to have their data erased is also given to users by the Act.⁵⁶ For a dating platform, it is assumed under this model that what happens to the sensitive data shared by the user is understood and controlled by the user. This data includes sexual orientation, religious identity, location and, more and more often, biometric data collected for verification. In commentary on the United States market, research is cited according to which most dating apps studied may share or sell users' personal data.⁵⁷ It is argued in this paper that a similar pattern may take hold in India unless data minimisation and purpose limitation are enforced by the Data Protection Board actively rather than only on complaint.⁵⁸ When "agree" is clicked by a user at sign-up, attention is focused on building a profile, not on reading a privacy policy. Little protection is given to the user's data by consent given at that moment once the data has been collected.

VIII. Grounding the Gap: Documented Incidents from India

The practical stakes of this gap can be understated if only legal analysis is relied on. Two incidents are set out in this Part. Both were reported by an established national newspaper on the basis of statements made by Delhi Police.

In January 2025, a twenty-three-year-old man from Shakarpur in East Delhi was arrested by Delhi Police. He had posed as a United States-based model on Bumble, Snapchat and WhatsApp. Photographs of a real Brazilian model and a virtual international mobile number were used by him. According to the police, over seven hundred women were contacted by him, private photographs and videos were obtained from them, and money was then extorted through threats to publish that material.⁵⁹ The investigation was started only in December 2024, when a complaint was filed by a university student who had met him on Bumble in January 2024. Three offences from Part V are shown in a single set of facts in this case: cheating by personation, misuse of another person's identity and sextortion. It is also shown how far a single unchecked identity can reach before it is detected. The pattern was carried on across three platforms and hundreds of victims for most of a year before the arrest was made.

In June 2024, an organised scheme run from a café on Vikas Marg in East Delhi was uncovered

⁵⁵ Digital Personal Data Protection Act, *supra* note 24, § 6.

⁵⁶ *Id.* § 12. 57

⁵⁷ Navarro, *supra* note 14.

⁵⁸ *Cf.* Goyal & Vyas, *supra* note 13.

⁵⁹ *Delhi Man Impersonates as Model from US*, *supra* note 12.

by Delhi Police. A civil services aspirant was contacted on Tinder through a profile in the name of “Versha”. According to the police, this profile was in fact run by a “table manager” employed by the café. The aspirant was then met by a woman using that name and was taken by her to the café to celebrate her birthday. She later left, and family problems were given as the reason. A bill of Rs. 1,21,917.70 was then presented to him by the café manager, and he was threatened and kept there until the payment was made online. A case of criminal conspiracy, cheating and robbery was registered under the Indian Penal Code, 1860, which was still in force at the time. One of the café’s owners and the woman were arrested. It was also stated by the Deputy Commissioner of Police that fake profiles are created on dating apps by such table managers to lure victims to cafés, and that victims are often kept from reporting by social stigma.⁶⁰ The pattern of extortion through manufactured intimacy described in Part V is shown by this case. A fake profile was placed before the victim through the platform’s own matching system, and its messaging system was used to bring him to the café. Yet no separate regulatory scrutiny was faced by the platform once the scheme was uncovered.

Both incidents were dealt with through ordinary criminal investigation after the harm had been done. In neither case was any legal consequence faced by the platforms involved. This outcome is consistent with the safe harbour law traced in Part VI. Neither case is presented as typical of the everyday experience of Indian dating-app users. These platforms are used by most people without any problem. The cases are presented because they were investigated by the police and reported by a national newspaper. Verifiable evidence of the harm patterns studied in this paper is therefore offered by each of them.

IX. Comparative Regulatory Models

Duties that go beyond the general intermediary rules have begun to be placed on dating and social platforms in other countries. Two models are examined in this Part. One is based on disclosure and the other on an active duty of care. The lessons offered by each model for Indian law are then considered.

9.1 United States: Disclosure-Based Regulation

One of the earliest disclosure laws for online dating in the United States was passed in Texas. The Internet Dating Safety Act was enacted through Senate Bill 488 and came into force on 1

⁶⁰ Hoque, *supra* note 12.

September 2011. It now forms Chapter 106 of the Texas Business and Commerce Code. Dating platforms are not required by this law to run background checks. Instead, every online dating service offered to Texas residents must tell its members, in a clear and visible way on its website, whether a criminal background check is run before members are allowed to talk to each other. A safety awareness notice, in which safer online dating practices are explained, must also be shown by every provider, whether or not checks are run. A breach can lead to a civil penalty sought by the state Attorney General.⁶¹ The aim of the law is explained in the committee report on the House companion bill. Few dating sites were checking users' criminal records, and users could choose more wisely if this information was given to them. The same report notes that similar disclosure rules already existed in some other states. An existing approach was therefore built on by Texas rather than a new one being invented.⁶²

A key advantage for India is offered by this disclosure model. The platform is not required to verify anyone's identity or background. It is only required to tell users honestly whether this is done. The choice is left with informed users, and no new system of mandatory surveillance is created.

9.2 United Kingdom: The Online Safety Act's Duty of Care

A different approach is taken by the United Kingdom's Online Safety Act, 2023. Pure safe harbour protection is replaced by an ongoing duty of care. "User-to-user services" are regulated by the Act. These are defined as internet services through which content generated by one user can be seen by other users.⁶³ Dating apps are covered by this definition. A risk assessment on illegal content must be carried out and kept up to date by every regulated service. In this assessment, the likelihood that the service will be used to commit crimes and the seriousness of the resulting harm are weighed. Proportionate measures must then be taken in response.⁶⁴ A further risk assessment focused on children must be carried out by services that are likely to be used by children.⁶⁵ These duties are enforced by Ofcom, the communications regulator. Penalties of up to eighteen million pounds or ten per cent of a company's qualifying worldwide

⁶¹ Tex. Bus. & Com. Code Ann. ch. 106, *supra* note 6.

⁶² House Comm. on Tech., Bill Analysis, *supra* note 16.

⁶³ Online Safety Act 2023, *supra* note 6, § 3.

⁶⁴ *Id.* §§ 9–10.

⁶⁵ *Id.* § 11.

revenue, whichever is greater, can be imposed by it.⁶⁶

When it is decided which measures are proportionate, the size, capacity and risk profile of each service are taken into account under the Act. One uniform standard is not applied to every service. This is the feature that can be borrowed most directly by India. The Indian dating market is made up of large international companies with strong compliance capacity as well as small domestic matrimonial start-ups with much less.

9.3 Lessons for India

Neither model would fit India if it were copied as a whole. A mandatory identity verification system would run into the proportionality concerns raised in *Puttaswamy*. After the Aadhaar judgment, limits on how Aadhaar authentication can be used by private companies would also be faced.⁶⁷ A duty of care system copied from the United Kingdom would need a regulator with the technical capacity of Ofcom. The Data Protection Board of India is still new, and capacity on that scale has not yet been shown by it.

The European Union's Digital Services Act, 2022 was also considered. Under that Act, hosting services are protected from liability for user content, much as under Section 79, and no general duty to monitor content is imposed. A notice-and-action system for reporting illegal content must be provided by them. Heavier duties, including a yearly assessment of systemic risks, are placed only on very large online platforms with more than forty-five million users in the European Union, and fines of up to six per cent of worldwide annual turnover can be imposed.⁶⁸ The Act has not been used as a main model in this paper for two reasons. Its basic liability rule is already close to the Indian position after *Shreya Singhal*. Its heaviest duties are also aimed at the largest platforms, and at the time of writing no dating app appears to have been designated as one of them. Less can therefore be learned from it for the specific problem of dating platforms than from the Texas and United Kingdom models.

What is shared by both models, and what is missing in India, is the recognition that a dating platform is not a passive host. The risk created by it is actively shaped through its matching algorithm, its messaging system and its choices about what safety information is shared with

⁶⁶ *Id.* sch. 13, para. 4.

⁶⁷ *Puttaswamy (Aadhaar)*, *supra* note 49.

⁶⁸ Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act), 2022 O.J. (L 277) 1, arts. 6, 8, 16, 33–35, 52, 74.

users. The disclosure idea of the Texas model and the proportionate, size-based idea of the United Kingdom model are both borrowed in India's reform path, which is set out in Part XI. Both are adapted to India's identity systems and institutional capacity.

X. Objections to Reform

A case for stronger duties on dating platforms must also answer the case against them. Three main objections are considered in this Part.

10.1 The Cost to Small Platforms

It may be argued that new duties would be too costly for small Indian matrimonial and dating start-ups, and that only large international companies would be able to meet them. If this happened, the market would be handed to the very companies that already hold the most user data. This concern is real, but it is met by the design of the reforms proposed in this paper. The core duty is one of disclosure. Only an honest statement of what checks are and are not carried out is required, and very little cost is involved in it. The heavier duties, such as a dedicated victim support channel, are proposed only for platforms above a notified user threshold. The same size-based approach is already followed in India for significant social media intermediaries and in the United Kingdom under the Online Safety Act.⁶⁹

10.2 The Risk of Over-Censorship

It may also be argued that wider platform liability would lead platforms to remove lawful profiles and messages simply to protect themselves. This was the concern behind *Shreya Singhal*, and it has been developed in academic writing on the liability of gatekeepers.⁷⁰ The concern is a serious one wherever speech is involved. But the reforms proposed in this paper do not ask platforms to judge whether content is lawful, and no new ground for removing content is created by them. They are aimed instead at the design of the platform: what checks are run, what users are told and how quickly complaints are handled. The Section 79 safe harbour for user content is left in place.

⁶⁹ IT Rules, *supra* note 21, r. 4(1); Online Safety Act 2023, *supra* note 6.

⁷⁰ *Shreya Singhal*, *supra* note 9; Arun, *supra* note 10.

10.3 The Safety of Vulnerable Users

The strongest objection concerns users who depend on privacy for their safety. Dating apps are an important space for LGBTQ+ users, and for some of them a hidden identity is a form of protection against family pressure, blackmail or violence. It has been documented by Human Rights Watch that dating apps have been used in several countries by the police and by private individuals to trap, extort and expose LGBT users.⁷¹ If every user were forced to link a profile to a legal identity, many people could be exposed at once by a single data breach or a single misuse of that data. The risk is greater for groups who already face more image-based abuse on dating apps, and whose sexual orientation is recognised in *Puttaswamy* as a protected part of privacy.⁷² For this reason, mandatory identity checks are not recommended in this paper. The disclosure model is preferred precisely because users can be protected by it without a new store of identity data being placed in the hands of private companies. Where verification is offered, it should remain optional, and platforms should be allowed to confirm that a user is a real person without keeping a record of who that person is.

XI. Recommendations

11.1 A Dating-Platform-Specific Due Diligence Code

The existing rule-making power under the Information Technology Act, 2000 should be used by the Central Government to notify a separate due diligence schedule for dating and matrimonial platforms.⁷³ At a minimum, three things should be required by this schedule. First, a working mobile number should be verified by a user before another user can be messaged. Second, photo verification should be made a condition for appearing in match results rather than an optional feature. Third, a standard safety notice should be displayed by each platform, in which it is stated exactly what verification is and is not carried out. Through this third requirement, the Texas disclosure model, including its safety awareness notice, is adapted to Indian conditions.⁷⁴ This schedule could be notified by the Ministry of Electronics and Information Technology under its existing rule-making power, so no new Act of Parliament

⁷¹ Human Rights Watch, “*All This Terror Because of a Photo*”: Digital Targeting and Its Offline Consequences for LGBT People in the Middle East and North Africa (Feb. 21, 2023).

⁷² Waldman, *Law, Privacy, and Online Dating*, *supra* note 18; *Puttaswamy*, *supra* note 48.

⁷³ Information Technology Act, *supra* note 20, §§ 79(2)(c), 87(2)(zg).

⁷⁴ Tex. Bus. & Com. Code Ann. ch. 106, *supra* note 6.

would be needed.

11.2 Mandatory Safety Disclosure, Not Mandatory Surveillance

A state-mandated background check for every user is not recommended in this paper. In line with *Puttaswamy*, such a requirement would be disproportionate to the privacy interests at stake.⁷⁵ Instead, platforms should be required by law to state clearly, before an account is created, whether any identity or criminal history checks are carried out and, if so, how. A choice could then be made by users between platforms with different safety standards, as is allowed under the Texas law. This duty could be placed in the same schedule, so that one set of rules is followed by all dating platforms.

11.3 A Dedicated Grievance and Victim-Compensation Mechanism

The general Grievance Officer system under the 2021 Rules should be supported, for dating platforms above a notified user threshold, by a dedicated victim support channel. Cases of catfishing, sextortion and platform-based extortion should be handled through this channel. Responses should also be given faster than within the general fifteen-day window, because sextortion threats are highly time-sensitive. The Data Protection Board of India should also be empowered by Parliament to direct platforms that repeatedly fail their due diligence duties to pay into a victim compensation fund.⁷⁶ Part of the legal costs faced by victims in pursuing criminal complaints against offenders who can be traced could be met from this fund. The dedicated channel could be required by the Ministry through the same rules, but an amendment to the Digital Personal Data Protection Act, 2023 would be needed for the compensation fund.

11.4 Calibrated, Deterrent Penalties

Penalties for breaking the due diligence duties of dating platforms should be linked to platform revenue rather than fixed at a flat amount. This approach is followed by the United Kingdom's Online Safety Act.⁷⁷ Under a penalty linked to revenue, real weight is felt by a large international platform, while a small domestic start-up is not crushed. The Board is already directed by the Digital Personal Data Protection Act, 2023 to consider factors such as the

⁷⁵ *Puttaswamy*, *supra* note 48.

⁷⁶ See Digital Personal Data Protection Act, *supra* note 24, §§ 27, 33 (setting out the Board's present powers).

⁷⁷ Online Safety Act 2023, *supra* note 6, sch. 13, para. 4.

nature, seriousness and length of a breach when a penalty is set.⁷⁸ This scaled approach should be extended through subordinate legislation to due diligence failures by dating platforms.

11.5 Public Legal Literacy Campaigns

Finally, victims are likely to be discouraged from reporting by a low awareness of legal remedies and by the shame of admitting that they were deceived through a dating platform. Targeted awareness campaigns should be run by state cyber crime cells. In these campaigns, the criminal provisions listed in Part V and the process for filing a complaint through the National Cyber Crime Reporting Portal should be explained in plain language.⁷⁹ The accountability gap cannot be closed by awareness alone. But it is a necessary addition to the structural reforms set out above. Even a well-designed legal remedy is of little use if it is not known to the victim. These campaigns could be supported by the Ministry of Home Affairs, by which the National Cyber Crime Reporting Portal is already run.

The five reforms, the bodies responsible for them and the time needed for each are summarised in Table 1.

Reform	Responsible body	Legal route	Timeline
Due diligence code for dating platforms	Ministry of Electronics and Information Technology	Rules under Sections 79(2)(c) and 87(2)(zg), IT Act, 2000	Short term (within one year)
Mandatory safety disclosure	Ministry of Electronics and Information Technology	Same schedule of rules	Short term (within one year)
Victim support channel and compensation fund	Ministry of Electronics and Information Technology; Parliament; Data Protection Board	Amendment to the IT Rules, 2021 and to the DPDP Act, 2023	Medium term (one to three years)
Revenue-linked	Central Government;	Subordinate	Medium term (one

⁷⁸ Digital Personal Data Protection Act, *supra* note 24, § 33(2).

⁷⁹ Ministry of Home Affs., National Cyber Crime Reporting Portal.

penalties	Parliament	legislation and statutory amendment	to three years)
Public legal literacy campaigns	State cyber crime cells; Ministry of Home Affairs	Executive action	Short term (within one year)

Table 1: Summary of Recommendations

XII. Conclusion

Online dating has become a mainstream way for people to meet in India. Yet the industry is still governed, in substance, by the general law of intermediaries, which was written for an internet of forums and marketplaces. The same conditional safe harbour under Section 79 of the Information Technology Act, 2000 is enjoyed by dating platforms as by any other website that carries user content. That law was built by the courts through the Bazeem.com litigation, *Shreya Singhal* and *Sharat Babu Digumarti*.⁸⁰ Romance fraud, catfishing and sextortion were not involved in any of these cases. All of them were aimed at protecting platforms from strict liability for content that could not reasonably be checked. That protection is still suitable for the ordinary hosting of user content. It fits poorly with a product that is designed to introduce strangers on the basis of an unchecked claim, and whose success is measured by how often that introduction leads to a meeting in person.

The resulting accountability gap has been traced in this paper across five areas. First, the safe harbour is used as a shield rather than as a standard of performance. Second, no duty is imposed by law to verify identity, or even to disclose whether identity is verified by a platform. Third, the deterrent value of the penalty system has not been tested against dating platforms. Fourth, harm enabled by platforms is made invisible in the national crime data. Fifth, a level of informed user control is assumed by the data protection framework that is not delivered by the sign-up process. The main objections to reform, based on cost, over-censorship and the safety of vulnerable users, have also been answered. It is shown by practice in the United States and the United Kingdom that a choice between privacy and safety is not required to close this gap.

Workable templates are offered by both the Texas disclosure model and the United Kingdom's proportionate duty of care. The proportionality standard set by the Supreme Court in

⁸⁰ *Avnish Bajaj*, *supra* note 8; *Shreya Singhal*, *supra* note 9; *Sharat Babu Digumarti*, *supra* note 44.

Puttaswamy is respected by both, and the information needed by users to protect themselves is given by both.⁸¹

The reforms proposed in Part XI are neither radical nor new. They are a due diligence code for dating platforms, mandatory safety disclosure instead of mandatory surveillance, a faster and better-resourced grievance system, penalties linked to revenue and sustained public legal awareness. Each of them is borrowed from a technique already tested elsewhere and is adapted to Indian conditions. Until such reforms are adopted by India, a person who is deceived, cheated or endangered through a dating platform will find that almost no separate legal responsibility is borne by the platform for what happened. The victim was introduced to the wrongdoer by that platform, and the data needed to identify that person is held only by it. In this sense, the victim is left by the law exactly where the victim was left by the platform: ghosted.

⁸¹ *Puttaswamy*, *supra* note 48.

Bibliography

A. Statutes and Rules (India)

Constitution of India.

Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

Bharatiya Nyaya Sanhita, 2023.

Consumer Protection Act, 2019.

Consumer Protection (E-Commerce) Rules, 2020.

Digital Personal Data Protection Act, 2023.

Digital Personal Data Protection Rules, 2025.

Information Technology Act, 2000.

Information Technology (Amendment) Act, 2008.

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

Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

Ministry of Electronics & Information Technology, Notification S.O. 942(E) (2021).

Motor Vehicle Aggregator Guidelines, 2025.

Protection of Children from Sexual Offences Act, 2012.

B. Cases

Aneeta Hada v. Godfather Travels & Tours (P) Ltd., (2012) 5 SCC 661.

Avnish Bajaj v. State (NCT of Delhi), 116 (2005) DLT 427.

Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

Justice K.S. Puttaswamy (Retd.) v. Union of India (Aadhaar), (2019) 1 SCC 1.

Navtej Singh Johar v. Union of India, (2018) 10 SCC 1.

Sharat Babu Digumarti v. Government (NCT of Delhi), (2017) 2 SCC 18.

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

C. Foreign Law and Legislative Materials

Online Safety Act 2023 (United Kingdom).

Regulation (EU) 2022/2065 on a Single Market for Digital Services (Digital Services Act), 2022.

Texas Internet Dating Safety Act, Tex. Bus. & Com. Code ch. 106 (2011).

Texas House Committee on Technology, Bill Analysis, C.S.H.B. 1052 (2011), <https://capitol.texas.gov/tlodocs/82R/analysis/html/HB01052H.htm>.

D. Reports

Human Rights Watch, *“All This Terror Because of a Photo”: Digital Targeting and Its Offline Consequences for LGBT People in the Middle East and North Africa* (2023), <https://www.hrw.org/report/2023/02/21/all-terror-because-photo/digital-targeting-and-itsoffline-consequences-lgbt>.

National Crime Records Bureau, *Crime in India 2023* (2025).

National Crime Records Bureau, *Crime in India 2024* (2026).

E. Articles and Websites

Ari Ezra Waldman, *Law, Privacy, and Online Dating: “Revenge Porn” in Gay Online Communities*, 44 Law & Soc. Inquiry 987 (2019), <https://doi.org/10.1017/lsi.2018.29>.

Ari Ezra Waldman, *Safe Social Spaces*, 96 Wash. U. L. Rev. 1537 (2019).

Bismah Malik, *Stupid Cupid: How Dating Apps in India Have Become Crime Epicentres*, Inc42 (2024), <https://inc42.com/features/stupid-cupid-how-dating-apps-in-india-have-become-crime-epicentres/>.

Chinmayi Arun, *Gatekeeper Liability and Article 19(1)(a) of the Constitution of India* (Centre for Communication Governance, NLU Delhi, Working Paper, 2015), <https://ssrn.com/abstract=2643278>.

Delhi Man Impersonates as Model from US, Blackmails Over 700 Women on Bumble, Snapchat with Private Photos, The Tribune (2025), <https://www.tribuneindia.com/news/delhi/delhi-manimpersonates-as-model-from-us->

blackmails-over-700-women-on-bumble-snapchat-withprivate-photos/.

Kiara J. Patiño Navarro, *Identity & Criminal Check Verification: Potential Solution to Bridging the Safety Gap in Dating Apps*, California Lawyers Association (2025), <https://calawyers.org/privacy-law/identity-criminal-check-verification-potential-solution-tobridging-the-safety-gap-in-dating-apps/>.

Nandita Goyal & Archit Vyas, *Ghosts in the Machine: Dating Apps and the DPDP Act*, Bar & Bench (2025), <https://www.barandbench.com/columns/ghosts-in-the-machine-dpdp-act>.

Samad Hoque, *App Date Turns Costly for Civil Services Aspirant*, The Tribune (2024), <https://www.tribuneindia.com/news/delhi/app-date-turns-costly-for-civil-services-aspirant635145>.

National Cyber Crime Reporting Portal, Ministry of Home Affairs, <https://cybercrime.gov.in>.