INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed



www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

Copyright © International Journal for Legal Research & Analysis. All rights reserved.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

DEEPFAKE TECHNOLOGY: LEGAL AND ETHICAL ISSUES IN DIGITAL INDIA

A Doctrinal and Analytical Study of Gendered Cyber Harms, Non-Consensual Intimate Imagery and Digital Rights

AUTHORED BY - SURESH KOMMU
LL.M. (Technology and Cyber Law) Scholar
Aurora Higher Education and Research Academy
(Deemed-to-be-University), Hyderabad, Telangana, India

Abstract

The rapid advancement of Artificial Intelligence (AI) and emerging digital technologies has transformed digital communication, content creation, and information sharing. However, these developments have also introduced serious legal and ethical challenges, particularly through the misuse of deepfake technology. deepfakes, generated using artificial intelligence techniques such as Generative Adversarial Networks (gans) and deep learning, enable the creation of highly realistic manipulated images, videos, and audio recordings. Among their most concerning applications are non-consensual sexual imagery, identity impersonation, image-based sexual abuse, online harassment, and gendered cyber harms, disproportionately affecting women and vulnerable individuals. Such practices threaten individual privacy, dignity, reputation, autonomy, and fundamental rights in the digital environment.

This paper examines the legal and ethical implications of deepfake technology in the Indian context, with particular emphasis on AI-generated non-consensual intimate imagery and gender-based digital violence. It analyses the constitutional dimensions of privacy and dignity under article 21 of the Indian constitution and explores the applicability of existing legal frameworks, including the Information Technology (IT) act, 2000, the Bharatiya Nyaya Sanhita, 2023, and the Digital Personal Data Protection act, 2023. The study further evaluates the challenges associated with victim identification, digital evidence, intermediary accountability, content removal, and effective enforcement mechanisms. Adopting a doctrinal and analytical research methodology, the paper highlights the limitations of existing regulatory approaches in addressing rapidly evolving AI-generated harms. It argues for a comprehensive, gender-sensitive legal framework that ensures accountability, strengthens victim protection,

ISSN: 2582-6433

promotes digital literacy, and establishes responsible AI governance while safeguarding constitutional freedoms in India's digital society.

Keywords: Artificial Intelligence; Deepfake Technology; Gendered cyber harms; non-consensual sexual imagery; Digital privacy; Cybersecurity; Legal and ethical issues.

1. INTRODUCTION

Artificial intelligence has changed how pictures voices and videos get made and shared these days. Tools can make fake versions that look like a real person doing or saying things that never happened. These are often called deepfakes when they come from machine learning especially neural networks. Some uses seem fine like in movies or for accessibility but the bad ones cause real problems for people and for trust in what we see.

The worst cases happen when someone face or voice gets put into sexual content without any agreement. Even if the whole thing is made up the effects feel very real for the person shown. They might deal with shame threats to their job or family and have to chase the images across sites while trying to show it is fake. It is hard to stop because copies spread so easily.

This kind of work looks at AI made non consensual intimate images and how they hit women more in India. It does not say every deepfake should be banned. Some things like satire or art that is clearly labeled should stay okay. The line matters because blocking everything would hurt free speech.

Indian laws have parts that can deal with some of this but they were not written for these new fakes. How they apply depends on what the material shows who made it the age of the person and what the platform does. That leaves things scattered so victims are not always sure where to go and results can vary.

The study tries to look at how these abuses touch privacy and dignity. It checks what the Constitution the IT Act the new criminal code and the data protection law can do. It also thinks about what platforms should handle when complaints come in and what evidence problems victims face. Some reforms might help without going too far on expression.

The approach is mostly reading laws and court cases rather than counting cases. It does not claim to know exactly how common this is. Claims about harm come from the rights involved and the way the conduct works. When the law is unclear on fully made up images the paper just notes that instead of acting like it is settled.

Making these images usually starts with grabbing source material then training a model to swap faces or voices. Things like GANs or other systems do the work. For law what matters is the

ISSN: 2582-6433

end result not the exact method. A fake intimate picture can come from swapping a face onto another body or just altering one photo.

Some common bad uses are non consensual sexual images voice clones for threats or people pretending to be someone else to get money or access. The paper stays mostly with those where consent and identity are the issue. The injury stays real even without an original photo because the persons identity gets used in a sexual way they never chose. It can get sent to bosses or relatives and used for blackmail. Women often face more of this because of how stigma works but others can be hit too.

The Constitution through Article 21 protects privacy and dignity after the Puttaswamy case. That links to control over personal info and choices about intimate life. Using someones face for fake sexual stuff takes that control away. Dignity covers more than physical harm it includes not letting others turn your identity into something public and false. Equality under Article 14 means systems should not put extra burdens on victims who have less help or face stigma. Free speech under Article 19 needs care so rules do not block parody or reporting.

It seems the current setup leaves gaps especially on fully synthetic stuff and on how platforms respond fast. Some parts feel like they could work better with clearer duties and easier ways for victims to get images down without proving everything again and again. That part gets a bit messy when evidence rules do not fit AI material well.

5. STATUTORY FRAMEWORK IN INDIA

5.1 Information Technology Act, 2000

The IT Act covers a lot of computer crimes and some parts might reach deepfake stuff depending on what happened. Section 66C deals with identity theft when someone uses another persons signature or password in a dishonest way. Section 66D covers cheating by pretending to be someone else through a device or computer. Those could matter if a fake voice or face is used to trick people for gain or something similar.

Section 66E is about taking or sharing private images without consent and it gets tricky with completely made up ones. The wording talks about capturing an actual private area so a fully synthetic image might not fit. It probably works better for edited photos but not every deepfake lands inside it. Some clarification from lawmakers would help.

Sections 67 and 67A look at obscene or sexually explicit material sent electronically and 67B is for anything involving kids. Those rules could apply to explicit deepfakes if the details match court views. Cases with minors need strong protection and the fact it is AI made should not change that.

ISSN: 2582-6433

Section 69A lets the government block access in certain cases while 69 and 79 give some protection to platforms for user content if they follow the rules. Those matter for how sites handle things but blocking alone does not fix the harm to victims or give them compensation.

The new Bharatiya Nyaya Sanhita has rules that might cover related behavior. Section 77 on voyeurism talks about watching or sharing private images of women and its reach to fabricated material is not clear. Section 78 covers stalking through online monitoring and 79 deals with insults to modesty or privacy intrusions. Other general crimes like cheating or defamation might fit in some situations but a deepfake by itself does not prove every element.

It feels like the law should not stretch old offences too far and a clearer rule on non consensual synthetic images would be better. That new offence could separate creation from distribution and threats and make extra penalties for targeting kids or repeated acts.

The data protection law treats faces and voices as personal data but it is not really a full criminal tool against deepfakes. The timing of when parts come into force means some obligations are not active yet so the framework is only partly useful right now. Even when running it mainly helps with commercial data handlers and may not catch every creator.

Recent changes to the intermediary rules require platforms to act fast on complaints about private or morphed content including AI versions. New rules on synthetic generated information add duties for labelling and checks on big platforms. Those steps recognise the risks but labels alone do not fix the lack of consent or stop the harm. Better removal processes and direct remedies against creators would make more difference.

6. JUDICIAL APPROACH AND EMERGING PRINCIPLES

6.1 K.S. Puttaswamy (Retd.) v. Union of India

The nine-judge decision in Puttaswamy is the constitutional foundation for privacy-based analysis. It recognises privacy as intrinsic to life, liberty and dignity and explains that privacy protects individual autonomy and personal choices.[13] Its significance for deepfakes is that privacy cannot be reduced to secrecy about authentic facts. The appropriation and synthetic manipulation of identifying features can interfere with the individual's ability to control intimate self-presentation.

6.2 Shreya Singhal v. Union of India

In Shreya Singhal v. Union of India, the Supreme Court read down the intermediary safe-harbour provision's "actual knowledge" requirement in the context then before it, holding that an intermediary's obligation under section 79(3)(b) was triggered by a court order or

ISSN: 2582-6433

notification by the appropriate government or its agency, rather than an intermediary's unilateral assessment of illegality.[14] The decision sought to avoid private intermediaries deciding complex questions of legality at scale and to protect speech from arbitrary removal.

The 2021 Rules and subsequent amendments provide more specific complaint-based procedures, including the special twenty-four-hour route for intimate or impersonation content. The legal framework must be read as a whole: the statutory safe-harbour provision, judicial interpretation, and valid subordinate legislation all matter. A victim-facing system should make the complaint route clear while retaining safeguards against malicious or mistaken takedown requests.

6.3 Anil Kapoor v. Simply Life India

In Anil Kapoor v. Simply Life India, the Delhi High Court considered unauthorised use of the plaintiff's name, image, voice and persona, including AI-generated and morphed material and fake pornographic depictions. The Court granted interim protection against specified misuse of his personality attributes through technological tools, including AI and deepfakes.[15] The case demonstrates judicial willingness to protect personality interests and dignity against technologically enabled appropriation.

The decision is useful but should not be overstated. It arose in a celebrity personality-rights action and does not establish a comprehensive statutory cause of action for every victim of intimate-image abuse. Ordinary individuals may lack the resources to bring a civil suit, identify anonymous defendants or obtain broad injunctions. A general victim-protection regime must therefore be accessible beyond high-profile claimants.

7. KEY LEGAL AND PRACTICAL CHALLENGES

7.1 Fragmented Offence Coverage

The first challenge is the absence of a single, clearly defined offence addressing the creation and distribution of non-consensual synthetic intimate imagery. Existing provisions may apply to identity theft, personation, obscenity, voyeurism, stalking, intimidation or defamation, but each has separate elements. The gap is particularly visible where the image is entirely generated and no authentic private-area image was captured.

7.2 Attribution and Anonymity

Deepfake production may involve several actors: the person who supplies source images, the person who operates a model, the person who edits the output, the account that first uploads it, and users who knowingly redistribute it. Accounts may be anonymous, disposable or located

ISSN: 2582-6433

outside India. Identifying the original creator can require platform records, subscriber information, device data and cross-border cooperation. Investigators must distinguish the creator from a person whose account was compromised or whose content was reposted without knowledge.

7.3 Digital Evidence and Authentication

Synthetic content creates evidentiary complexity because visual appearance is no longer a reliable indicator of authenticity. A victim may need to preserve the URL, account identifier, timestamps, message headers, original files, screenshots, metadata, platform complaint numbers and communications containing threats. Investigators may require forensic imaging, hash values, chain-of-custody records and expert analysis. A screenshot alone may be useful but can be incomplete or challenged.

The Bharatiya Sakshya Adhiniyam, 2023 governs the admissibility of electronic and digital records. Its electronic-record provisions and certification requirements must be followed where applicable.[16] Investigators should preserve the original electronic record and relevant device or platform data, document each transfer and avoid editing files in a way that destroys metadata. Courts should also be alert to the possibility that a purported recording is synthetic, altered or taken out of context.

7.4 Speed of Dissemination and Replication

A removal order directed at one URL may not prevent copies from appearing on other accounts, mirror sites or messaging groups. Victims may be required to file repeated complaints, which can deepen distress and prolong exposure. Effective response requires a process for identifying substantially identical copies, preventing re-uploads where technically feasible, and providing a single point of contact for status updates.

7.5 Platform Accountability and Due Process

Platforms possess technical information and control over hosting, recommendation and account systems. They are therefore central to prevention and response. At the same time, automated detection can generate false positives, particularly for journalism, education, consensual adult content, satire and documentation of abuse. Platform duties should be specific, auditable and proportionate, with notice, reasoned decisions and appeal procedures where consistent with urgent victim protection.

ISSN: 2582-6433

7.6 Victim Identification, Stigma and Access to Justice

Victims may hesitate to approach police or platforms because they fear blame, exposure or further circulation of the material. A complaint process that requires the victim to repeatedly upload intimate content can itself reproduce the harm. Reporting mechanisms should allow secure submission, restricted access, minimal disclosure and representation by an authorised person. Police personnel should receive training on synthetic media, gender-sensitive interviewing and preservation of digital evidence.

8. ETHICAL DIMENSIONS AND RESPONSIBLE AI GOVERNANCE

8.1 Consent and Identity Autonomy

Consent to share an ordinary photograph is not consent to transform it into sexual material. Nor does public availability of a photograph amount to a waiver of privacy or a licence to create a false intimate depiction. Ethical design should treat biometric and identity-related material as high-risk when used to generate realistic depictions of identifiable persons.

8.2 Bias, Power and Gender

AI systems can reproduce social bias in their training data, design and deployment. The impact of non-consensual sexual deepfakes is shaped not only by model performance but also by existing inequalities, sexual stigma and unequal access to remedies. Ethical governance should therefore include gender-impact assessment, consultation with affected communities, accessible reporting and independent evaluation of safety measures.

8.3 Transparency, Provenance and Labelling

Provenance systems, cryptographic credentials, watermarking and metadata can help identify the origin or editing history of synthetic content. These measures are useful but imperfect: metadata can be stripped, watermarks can be altered, and detection tools can produce errors. A provenance indicator should not be treated as conclusive proof that content is authentic or inauthentic. It should operate as one layer in a broader accountability system.

8.4 Balancing Innovation and Protection

Responsible AI governance should preserve beneficial uses of synthetic media. A filmmaker's disclosed visual effect, a satirical impersonation, an accessibility tool or a consensual voice clone should not be equated automatically with abusive impersonation. Regulation should focus on consent, deception, context, intent, foreseeable harm and public interest. A narrow,

ISSN: 2582-6433

clearly drafted law is more defensible than broad restrictions based on the mere use of AI.

9. PROPOSED REFORMS: A GENDER-SENSITIVE LEGAL MODEL

9.1 Enact a Specific Offence for Non-Consensual Synthetic Intimate Imagery

Parliament should consider a technology-neutral offence covering the knowing creation, publication, transmission, distribution or threatened distribution of an identifiable person's intimate depiction without consent, where the conduct is intended to cause harm, intimidate, harass, obtain an advantage or where the accused knows or ought reasonably to know that serious harm is likely. The definition should expressly include wholly synthetic, digitally altered and composited depictions, whether or not an authentic intimate image exists.

The offence should distinguish levels of culpability. Creation for private experimentation without dissemination may require a different response from deliberate publication, extortion, commercial sale or repeated distribution. Aggravating circumstances should include depiction of a child, threats, extortion, repeated targeting, organised distribution, abuse of authority and distribution for commercial gain. The law should avoid criminalising legitimate satire, art, journalism or public-interest expression where there is no non-consensual intimate abuse and adequate contextual safeguards apply.

9.2 Establish a Rapid, Victim-Centred Removal Procedure

A unified reporting mechanism should allow a victim or authorised representative to report a non-consensual intimate deepfake through a secure portal. Platforms should acknowledge the complaint promptly, provide a tracking number, assess the material using trained human reviewers supported by technical tools, and communicate a reasoned outcome. The existing twenty-four-hour route under the IT Rules should be operationalised through standardised forms and clear escalation channels.

The system should include preservation of relevant evidence before removal, subject to privacy and security safeguards. It should also support repeat-upload mitigation through perceptual hashes or other privacy-preserving matching technologies, with human review to reduce erroneous blocking. The victim should not be required to make the content more widely available merely to prove the complaint.

9.3 Strengthen Investigation and Digital Forensics

Specialised cybercrime units should receive training on deepfake detection, source tracing, platform preservation requests, electronic evidence and trauma-informed engagement.

ISSN: 2582-6433

Standard operating procedures should specify how to preserve original files, record URLs and timestamps, obtain forensic copies, document hash values, and request relevant platform records through lawful channels. Expert reports should explain both the methods used and their limitations.

9.4 Clarify Intermediary Duties and Accountability

The 2026 SGI framework should be complemented by transparent compliance reporting. Platforms should publish aggregate data on complaints involving non-consensual intimate imagery, median response times, repeat uploads, appeals, reinstatements and enforcement errors. Large platforms should maintain accessible grievance officers and escalation pathways. Any automated detection obligation should be risk-based, technically realistic and accompanied by safeguards for lawful speech.

9.5 Provide Civil Remedies, Compensation and Support

Criminal prosecution alone cannot repair the injury. Victims should have accessible routes to injunctions, damages where legally available, correction or removal orders, and protection against further disclosure. Legal aid, counselling and digital-safety assistance should be available without requiring the victim to establish that the deepfake was believed by every recipient. Courts should consider confidentiality directions and pseudonymisation where appropriate.

9.6 Digital Literacy and Public Awareness

Schools, universities, workplaces and public institutions should teach consent, image-based abuse, synthetic-media literacy and safe reporting. Public campaigns should explain that forwarding or reposting abusive material can perpetuate harm. Training should also address the limits of deepfake detectors so that victims are not dismissed merely because a tool fails to identify manipulation.

9.7 Independent Oversight and Rights-Based Safeguards

A specialist oversight mechanism or designated authority could issue model procedures, coordinate cross-platform complaints and publish anonymised trend reports. Its powers should be clearly defined by law and subject to judicial review. Decisions affecting expression should be reasoned, reviewable and proportionate. Independent audits should assess whether detection systems disproportionately flag particular groups, dialects, appearances or forms of expression.

ISSN: 2582-6433

10. DISCUSSION: THE CASE FOR A COHERENT RIGHTS-BASED RESPONSE

The analysis demonstrates that India's legal framework has evolved beyond a purely technology-neutral approach. The IT Act provides offences for privacy violations, personation and sexually explicit electronic material; the BNS addresses voyeurism, stalking and other offences against women; the IT Rules establish complaint and intermediary duties; and the 2026 amendments expressly address synthetically generated information. Constitutional privacy jurisprudence supplies the rights-based foundation for State protection.

Nevertheless, the framework remains incomplete in at least four respects. First, the statutory fit of provisions such as section 66E of the IT Act and section 77 of the BNS is uncertain where the intimate depiction is wholly synthetic. Second, the victim's practical path is fragmented across police, platforms, courts and data-protection institutions. Third, content labelling and takedown obligations do not by themselves provide attribution, compensation or rehabilitation. Fourth, the law must reconcile rapid intervention with safeguards against over-removal and arbitrary censorship.

The proposed model therefore rests on four connected pillars: a clearly defined offence; a rapid and secure removal-and-preservation mechanism; specialised investigation and victim support; and proportionate platform and AI-governance obligations. Each pillar addresses a different part of the harm. Criminal law identifies culpable conduct; platform procedures limit ongoing dissemination; forensic systems support proof; and civil and social remedies assist recovery.

A further principle is that the victim should not bear the entire cost of technological uncertainty. The burden of establishing the technical origin of an image should not become a barrier to urgent interim protection. At the same time, final criminal liability must be established through fair procedures and reliable evidence. Interim content restrictions and criminal convictions serve different purposes and should not be conflated.

11. CONCLUSION

Deepfake technology presents both opportunities and serious risks. Its misuse to create and circulate non-consensual intimate imagery demonstrates how AI can transform a person's identity into a vehicle for harassment, coercion and gendered digital violence. The resulting harm is not unreal merely because the image is synthetic. It can violate privacy, dignity, autonomy and reputation, and can expose victims to continuing humiliation and social consequences.

ISSN: 2582-6433

Indian law provides several routes for addressing deepfake-related conduct, but the application of existing offences is fact-sensitive and, in wholly synthetic intimate-image cases, sometimes uncertain. The constitutional principles in Puttaswamy, the IT Act, the BNS, the DPDP framework and the 2021 IT Rules as amended in 2026 together form an important foundation. They do not yet provide a single, comprehensive and accessible response to every form of non-consensual synthetic intimate imagery.

A balanced response should not prohibit deepfake technology as such. It should prohibit and remedy abusive conduct, recognise the particular vulnerability created by synthetic sexual depictions, and impose clear duties on actors who create, distribute or host unlawful material. A specific statutory offence, victim-centred takedown process, evidence-preservation standards, trained cybercrime personnel, civil remedies, digital literacy and transparent platform accountability are essential components of such a framework. The ultimate objective is a digital environment in which innovation and freedom of expression coexist with meaningful protection of consent, dignity and fundamental rights.

DEEPFAKE TECHNOLOGY: LEGAL AND ETHICAL ISSUES IN DIGITAL INDIA

1. INDIA CONST. art. 21.
2. K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).
3. Id.; see also R. Rajagopal v. State of Tamil Nadu, (1994) 6 S.C.C. 632 (India).
4. Information Technology Act, No. 21 of 2000, §§ 66C–66D, INDIA CODE (2000).
5. Bharatiya Nyaya Sanhita, No. 45 of 2023, § 77, INDIA CODE (2023).
6. Notification No. G.S.R. 843(E), Gazette of India, pt. II, sec. 3(i) (Nov. 13, 2025) (Digital Personal Data Protection Act, 2023 commencement notification).
7. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r. 3(2)(b), G.S.R. 139(E), Gazette of India, pt. II, sec. 3(i) (Feb. 25, 2021), as amended.
8. Ministry of Electronics & Information Technology, Government of India, Frequently Asked Questions on the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, at 1–2 (Feb. 10, 2026).
9. Puttaswamy, (2017) 10 S.C.C. 1.
10. Shreya Singhal v. Union of India, (2015) 5 S.C.C. 1 (India).
11. Anil Kapoor v. Simply Life India, CS(COMM) 652/2023, I.A. 18237/2023 (Delhi High Ct. Sept. 20, 2023) (order on interim injunction).

ISSN: 2582-6433

12. Bharatiya Sakshya Adhiniyam, No. 47 of 2023, §§ 61–63, INDIA CODE (2023).
13. INDIA CONST. arts. 14, 19(1)(a), 19(2), 21.
14. Information Technology Act, No. 21 of 2000, §§ 66C–66E, 67–67B, 69A, 79, INDIA CODE (2000).
15. Bharatiya Nyaya Sanhita, No. 45 of 2023, §§ 318, 336, 351, 356, INDIA CODE (2023) (potentially relevant depending on statutory elements and facts).
16. Digital Personal Data Protection Act, No. 22 of 2023, INDIA CODE (2023).
17. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, G.S.R. 120(E), Gazette of India, pt. II, sec. 3(i) (Feb. 10, 2026).
18. Ministry of Electronics & Information Technology, supra note 12.
19. R. Rajagopal v. State of Tamil Nadu, (1994) 6 S.C.C. 632 (India).
20. Shreya Singhal v. Union of India, (2015) 5 S.C.C. 1 (India).
21. Anil Kapoor v. Simply Life India, CS(COMM) 652/2023 (Delhi High Ct. Apr. 30, 2024) (final decree against certain defendants).

SELECTED BIBLIOGRAPHY

Primary Sources

THE CONSTITUTION OF INDIA.

Bharatiya Nyaya Sanhita, No. 45 of 2023, INDIA CODE (2023).

Bharatiya Sakshya Adhiniyam, No. 47 of 2023, INDIA CODE (2023).

Digital Personal Data Protection Act, No. 22 of 2023, INDIA CODE (2023).

Information Technology Act, No. 21 of 2000, INDIA CODE (2000).

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E), Gazette of India, pt. II, sec. 3(i) (Feb. 25, 2021), as amended.

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, G.S.R. 120(E), Gazette of India, pt. II, sec. 3(i) (Feb. 10, 2026).

Notification No. G.S.R. 843(E), Gazette of India, pt. II, sec. 3(i) (Nov. 13, 2025) (DPDP Act commencement).

Cases

Anil Kapoor v. Simply Life India, CS(COMM) 652/2023 (Delhi High Ct. Sept. 20, 2023).

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

R. Rajagopal v. State of Tamil Nadu, (1994) 6 S.C.C. 632 (India).

ISSN: 2582-6433

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

Government and Policy Materials

Ministry of Electronics & Information Technology, Government of India, Frequently Asked Questions on the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026 (Feb. 10, 2026).

Ministry of Electronics & Information Technology, Government of India, Digital Personal Data Protection Rules, 2025 (Nov. 14, 2025).

Press Information Bureau, Government of India, India Well-Equipped to Tackle Evolving Online Harms and Cyber Crimes (Aug. 8, 2025).

IJLRA