Page: 392-421 *URL: www.lijdlr.com*

LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

ISSN: 2583-7753

LawFoyer International Journal of Doctrinal Legal Research

[ISSN: 2583-7753]

Volume 4 | Issue 2

2026

DOI: https://doi.org/10.70183/lijdlr.2026.v04.166

REGULATING ARTIFICIAL INTELLIGENCE AND DEEPFAKES IN INDIA: A LEGAL ANALYSIS OF PRIVACY, PLATFORM LIABILITY, CYBERCRIME, AND CONSTITUTIONAL FREE SPEECH

Ishani Chhaudha[1]

I. ABSTRACT

Artificial intelligence has evolved from a computational tool into a powerful medium of expression shaping identity, political communication, advertising, and social interaction. Deepfakes, synthetic audio, face swaps, voice cloning, and other forms of generative media create legal harms that intersect with privacy, defamation, fraud, cybercrime, intermediary liability, electoral integrity, and constitutional free speech. This article examines how the existing Indian legal framework including the Information Technology Act, 2000, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, the Digital Personal Data Protection Act, 2023, the Bharatiya Nyaya Sanhita, 2023, and constitutional jurisprudence under Justice K.S. Puttaswamy v. Union of India and Shreya Singhal v. Union of India can be interpreted to regulate harmful synthetic media. Using a doctrinal and analytical methodology, the article distinguishes between legitimate uses of artificial intelligence in satire, education, accessibility, and artistic expression, and malicious deepfakes that infringe dignity, facilitate impersonation, mislead voters, enable cyber fraud, or threaten public safety. It argues that India should adopt a rights-based regulatory framework grounded in informed consent, data protection, platform due diligence, forensic evidence preservation, proportionate labelling, effective grievance redressal, victim remedies, and court-reviewable takedown mechanisms. The article concludes that artificial intelligence and deepfakes can be effectively regulated within India's existing constitutional and statutory framework without undermining freedom of speech and democratic values.

II. KEYWORDS

Artificial Intelligence, Deepfakes, Privacy, Intermediary Liability, Cybercrime.

[1] Asian Law College, Ccs University (India). Email: ishani.chhaudha@gmail.com

 (ISSN: 2583-7753)

III. INTRODUCTION AND RESEARCH PROBLEM

AI is not in the background of data analytics and automation anymore. It has been brought to the surface of social life by artificial images, voices, video, chatbots, recommender algorithms and text generators. This process is particularly difficult with deepfakes, since they do not simply add a bit of false information to the record; it lies about the existence of a physical body. An individual can be portrayed as saying something that they never said, doing something that they have never done, promoting something of which they have never used, appearing in a sexual scene which they never agreed to and making a political endorsement of which they have never made. This damage is not merely informational in nature. It is a usurpation of the probity of vision and audition, a distortion of that, a technological attack upon it.

In India, the implications are grave because digital media are integral to democratic elections, the consumer economy, education, banking, work, leisure, and relationships. A deepfake could be used to perpetrate a cyber-crime, harass a woman by sharing non-consensual nude images, blackmail a student, harass a journalist, influence voters, impersonate a government official, trick an elderly person with cloned voice, or tarnish a company's reputation. These are harms that are committed within a legal framework that is not tailored to generative AI. The Information Technology Act, 2000 is the cyber law, and intermediary obligations are governed by the IT Rules. Privacy is constitutionally protected (post-Puttaswamy), data protection is enshrined in the Digital Personal Data Protection Act, 2023 and criminal liability is enshrined in the Bharatiya Nyaya Sanhita, 2023.[2]

Despite the increasing use of artificial intelligence and generative technologies, India does not yet have a dedicated statutory framework specifically regulating deepfakes and other forms of synthetic media. The existing legal response is dispersed across privacy law, cybercrime legislation, intermediary regulation, data protection law, and constitutional free speech jurisprudence. This fragmented framework creates uncertainty regarding the distinction between legitimate synthetic expression and unlawful deepfakes involving impersonation, fraud, sexual exploitation, and electoral

[2] Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

manipulation. The central research problem addressed in this article is whether the current Indian legal framework is sufficient to regulate deepfake related harms effectively while preserving privacy, dignity, and the constitutional guarantee of freedom of speech and expression.

India needs to pursue a multi-pronged strategy, rather than an outright prohibition. The legal issues related to privacy are consent, personhood, data mining, biometric manipulation, and personal attributes. The platform liability deals with the notice, removal, classification, redressal, amplification by algorithms, and retention of evidence. The law of cybercrime encompasses fraud, identity theft, sexual exploitation, fraud, harassment and child sexual abuse. The constraints outlined in constitutional law include legality, necessity, proportionality, reasonable restriction, protection and judicial review protections in the form of procedures. The issue is not only the regulation of AI, but the regulation of AI without interfering with the freedom of speech and creating an unrepresentative censorship regime.

A. Research Objectives

1. To examine the legal and constitutional challenges posed by artificial intelligence-generated deepfakes in India, particularly in relation to privacy, intermediary liability, cybercrime, and freedom of speech.
2. To analyse the adequacy of existing Indian laws, including the Information Technology Act, 2000, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, the Digital Personal Data Protection Act, 2023, and the Bharatiya Nyaya Sanhita, 2023, in addressing harms caused by deepfakes.
3. To distinguish between legitimate uses of synthetic media for satire, education, accessibility, and artistic expression, and unlawful uses involving impersonation, fraud, sexual exploitation, and electoral deception.
4. To propose a rights-based regulatory framework that balances privacy, dignity, victim protection, platform accountability, and constitutional free speech

B. Research Questions

1. To what extent does the existing Indian legal framework adequately regulate deepfakes and other forms of AI-generated synthetic media?
2. How should Indian law distinguish between constitutionally protected synthetic expression and harmful deepfakes that infringe privacy, dignity, and democratic integrity?
3. What duties should intermediaries and AI platforms bear in preventing, detecting, and responding to deepfake-related harms?
4. What legal and policy reforms are necessary to develop a constitutionally compliant and rights-based regulatory framework for artificial intelligence and deepfakes in India?

C. Research Methodology

This study adopts a doctrinal and analytical methodology. It examines primary legal sources, including the Constitution of India, the Information Technology Act, 2000, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, the Digital Personal Data Protection Act, 2023, the Bharatiya Nyaya Sanhita, 2023, and the Bharatiya Sakshya Adhiniyam, 2023. The research also analyses judicial precedents such as Justice K.S. Puttaswamy (Retd.) v. Union of India, Shreya Singhal v. Union of India, and Anuradha Bhasin v. Union of India. Secondary sources include scholarly articles, policy reports, and international regulatory instruments, including the European Union Digital Services Act and AI Act. A limited comparative approach is employed to identify best practices relevant to the Indian constitutional and regulatory context.

IV. THINKING ABOUT DEEPFAKES: FALSE SPEECH AND SYNTHETIC PERSONAE

A deepfake is not just a lie in the digital age. It is a synthetic portrayal that plays upon the markers that human beings use to recognise presence, truth and agency. Defamation law is concerned with statements that decrease reputation. Privacy law deals with privacy, disclosure and autonomy. Cybercrime law deals with

unauthorised access, cheating, identity theft and obscene or sexually explicit material. Deepfakes incorporate all of these but also involve a new feature: the apparent involvement of the victim in a simulated action. Typically, the victim is not only spoken about; the victim is also technologically made to speak and act.[3]

This makes the regulation of deepfakes more difficult than regulation of misinformation. A hoax written post can be countered with speech, factchecking, and defamation laws. But a convincing video or recorded voice message can circulate via messaging before it is fact checked. Although later proven false, the impact on dignity, reputation and psychological well-being may have been realised. The target may have to prove the negative: that the voice, face or body presented is not real. The shift in the burden of proof is a serious consequence of synthetic media.

Deepfakes also transform the concept of consent. Consent does not end when a person takes a photo, speech, or performance publicly available. An image of a person may be publicly available for viewing, use in criticism, or news reporting, but this does not mean that the image can be used to create a synthetic porn video, an investment fraud, a political endorsement, or a public provocation. This is also true of voice recordings, headshots, public speeches, YouTube clips and biometric data. Public is not the same as permission for synthetic use.[4]

This distinction is grounded in Indian privacy law. Puttaswamy acknowledges privacy as a facet of dignity, autonomy, and informational autonomy. It does not restrict privacy to secrecy. An individual can have a right to privacy even in relation to publicly visible data or attributes if the subsequent use alters the context, purpose, and implications of that information. This is the case with deepfake abuse. The face is on display, but the assumed face is not. The law should therefore protect contextual integrity, not confidentiality.

[3] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Gazette of India, pt. II, sec. 3(i) (Feb. 25, 2021).
[4] Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

V. EXISTING INDIAN LEGAL FRAMEWORK

India does not yet have a stand-alone law dedicated to artificial intelligence or deepfakes. It is spread across cyber law, data protection law, criminal law, intellectual property law, election law, consumer protection law, media law and constitutional law. This is not a problem in and of itself. Many harms arising from AI are best addressed via sector-specific rules because the use of deepfakes for sexual abuse is not the same as a deepfake used for product impersonation or satire. The problem is with fragmentation, lack of consistent remediation, lack of clarity and lack of capacity.[5]

The Information Technology Act, 2000 is important because deepfakes are made, stored, transmitted and published through computer resources. Sections relating to privacy, publishing or transmitting obscene or sexually explicit material, child sexual abuse material, preservation of information by intermediaries, and blocking of public access to information may apply depending on the facts. Section 69A and the Blocking Rules are also relevant because unlawful deepfake content may be blocked in the interests articulated in law, but also for procedural reasons because blocking impacts free speech and access to information.

The IT Rules contain due diligence requirements for intermediaries. They mandate that intermediaries publish rules and privacy policies, notify users not to host certain kinds of unlawful content, designating a grievance officer (where appropriate), and comply with lawful orders or notices within the specified framework. The post-Shreya Singhal position remains important from a constitutional perspective: intermediary liability cannot be tied to platforms independently judging illegality in each instance. Actual knowledge for removal, in the constitutionally safe form, is tied to information from court orders or government notifications, not just private individuals. This ensures that platforms are not left as private censorship enforcers while still allowing for legal removal.[6]

In addition to the statutory framework, the Ministry of Electronics and Information Technology (MeitY) issued important advisories in November and December 2023

[5] Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023 (India).
[6] Shreya Singhal v. Union of India, (2015) 5 SCC 1.

directing intermediaries to address the growing misuse of deepfakes and AI-generated misinformation. These advisories emphasised that intermediaries must comply with Rule 3(1)(b) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 by informing users not to host, display, upload, modify, publish, transmit, store, update, or share content that impersonates another person, contains materially deceptive information, or otherwise violates applicable law. Particular attention was drawn to Rule 3(1)(b)(v), which addresses impersonation, and Rule 3(1)(b)(vii), which covers false or misleading information capable of deceiving users. The advisories also directed platforms to act expeditiously on unlawful content, provide accessible grievance mechanisms, and ensure that terms of service clearly prohibit such misuse. Although these advisories do not create a separate deepfake statute, they represent the most explicit governmental articulation to date of intermediary responsibilities concerning synthetic media and demonstrate that existing regulatory powers are being adapted to respond to emerging harms caused by artificial intelligence generated content.

The Digital Personal Data Protection Act, 2023 introduces a privacy and data-governance element. Creating deepfakes sometimes requires personal data, including photos, audio and video, location data, profile details and sometimes biometric data. When such data is processed in the digital environment, the principles of purpose, notice, consent, legitimate use, security and accountability may apply. The DPDP regime does not on its own provide a comprehensive deepfake solution, but it can help clarify why unauthorised data scraping, reuse, profiling and synthetic use of personal data may be objectionable.

The Bharatiya Nyaya Sanhita, 2023 applies where deepfakes are used in cheating, forgery, criminal intimidation, defamation, sexual harassment, public mischief, and offences against public tranquillity. The offence will vary. A deepfake recommendation for an investment can be examined from cheating and impersonation. A deepfake sex video could raise issues of sexual privacy, obscenity, harassment and defamation. A forged speech by a religious or political leader may involve public order or enmity laws (if the criteria are satisfied). But criminal law must

not be an overkill because imprecise punishment of false and offensive online content will bring back the constitutional flaws witnessed in Shreya Singhal.

VI. PRIVACY, DIGNITY, AND INFORMATIONAL SELF-DETERMINATION

The violation of privacy in deepfakes is not just unauthorised access to private information. It also includes identity theft, loss of control over public persona, humiliation, non-consensual sexualisation, reputational damage and insecurity. Indian constitutional law is well poised to grasp these harms in light of the fact that privacy after Puttaswamy encompasses bodily privacy, informational privacy, autonomy, dignity, and autonomy over identity. Deepfakes harm all of these interests. This is particularly the case with the creation of synthetic intimate images, because the victim experiences social stigma without disclosure.[7]

Accordingly, a consent-based approach must distinguish between the creation and dissemination of synthetic intimate imagery and other forms of image manipulation. Consent to be photographed is not consented to be sexualised. Consent to record a performance is not consent to political parody. Consent to provide a voice sample to a service is not consent to voice cloning for fraud. Data protection law can help here by ensuring that processing is specific, informed and for a specific purpose. Our legal system should take account of the fact that personal data used to make a deepfake is not just data; it is connected to a person's dignity.

The right to privacy also demands positive institutional design. Victims must have rapid reporting mechanisms, evidence preservation, takedown mechanisms and forensic assistance. A deepfake allegation can't be just a private matter between the victim and the uploader. Companies, police, cyber cells, and the judiciary must respond without blocking legitimate speech. The threshold should be higher for non-consensual sexual deepfakes, child sexual abuse material, impersonations for fraud and targeted threats. Here, time is a factor of harm.[8]

[7] R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632.
[8] Information Technology Act, 2000, § 66D, No. 21, Acts of Parliament, 2000 (India).

However, privacy should not be an automatic shield against criticism, satire, investigative reporting, or reporting in the public interest. Public figures don't lose their privacy, but their privacy must be weighed against the public interest. Consent, deception, harm and context should determine the legal difference. A parody of a public figure should not be treated like a falsified video that is being released to mislead voters. A news article about the existence of a deepfake should not be treated like a deliberate republishing. So, context-sensitive regulation is important.

VII. PLATFORM RESPONSIBILITY AND THE LIMITS OF INTERMEDIARY REGULATION

Deepfakes most often go wrong not just because they are produced, but because they are shared, promoted, recommended, monetised, and re-uploaded over and over again. Intermediaries have control over key elements of this chain: user verification, moderation, ranking algorithms, advertising decisions, search rankings, metadata retention, grievance and repeat-offender policies. So, platform accountability is inevitable. However, the Indian Constitution demands such accountability should not make intermediaries unrepresentative speech legality judges.[9]

The Supreme Court's Shreya Singhal interpretation of intermediary liability is crucial. It acknowledged that online speech must not be chilled by putting private intermediaries in the position of determining vague legal questions with the threat of liability. This remains crucial in deepfake scenarios. A host may be expected to take prompt action on unequivocally unlawful content like non-consensual intimate deepfakes, child sexual abuse, fraud and court orders. However, vague calls to remove deceptive or offensive AI content without legal criteria may result in over-removal, political censorship and censorship of legitimate speech.

An alternative approach is graduated due diligence. Companies should have clear user policies against non-consensual intimate deepfakes, impersonation, fraud, child sexual abuse material and law-breaking AI content. They should have easy-to-access complaint mechanisms and trained moderation for high-impact areas. They should

[9] Information Technology Act, 2000, §§ 67, 67A, No. 21, Acts of Parliament, 2000 (India).

retain metadata and other material for lawful investigations. They should employ proportionate labelling or provenance for synthetic media if possible. They should offer redress for users whose content is removed. This approach offers victim protection and due process.[10]

The law also needs to cater for virality. An injunction to remove a video from only a single URL may not be effective, given that it can be replicated on multiple platforms and messaging apps. But proactive filtering is risky, given the use of fallible automated tools. The best solution is a hash matching and notice-based system for identical or highly similar unlawful content (especially for intimate deepfakes and child abuse material) and human moderation for borderline speech. They should also be obliged to not monetise or amplify through paid promotion any reported synthetic impersonation while it is under review.

Overseas law provides insight but can't be mimicked. The Digital Services Act of the European Union emphasises systemic risk, transparency, trusted flaggers and very large online platforms. The EU AI Act deals with AI risk types and transparency. India has different circumstances due to language diversity, election cycles, the prevalence of messaging apps, some instances of low media literacy, and variable police training. However, the principles of transparency, proportionality, traceability and remedy apply.

VIII. CYBERCRIME, CRIMINAL LAW AND PROOF

Abuse of deepfakes may only come to the attention of law enforcement once the damage is done. Cybercrime reports may relate to fraudulent investment videos, voice-cloned family crises, morphed intimate videos or photos, falsely confessed statements, AI-generated blackmail, public official impersonations, or social media manipulations. The first issue for law enforcement is storage. Digital evidence is fragile. User information, device logs, IP addresses, hashes, payments, metadata and

[10] Information Technology Act, 2000, § 67B, No. 21, Acts of Parliament, 2000 (India).

account reset information may be lost rapidly if not retained by platforms following legitimate requests for information.[11]

Deepfakes should not be considered one crime. The harm should determine the charge. Cheating and impersonation laws may apply to fraudulent deepfakes. Sexual deepfakes may fall within obscene or pornographic transmission, privacy, harassment and child-protective law (if they involve minors). Political deepfakes could attract election law or public nuisance issues if thresholds are reached. Reputational attacks may give rise to defamation, but criminal defamation should be used with caution to avoid chilling free speech.

The law of evidence must evolve. Neither courts nor police can rely on video or audio being self-authenticating. The evidence's chain of custody, device identity, metadata, compression artifacts, forensic hash values, and forensic examination will be essential. The shift to the Bharatiya Sakshya Adhiniyam, 2023 stresses the importance of procedural meticulosity with electronic and digital records. Litigation involving deepfakes will demand forensic laboratories, procedures for collection, and judicial understanding of probabilistic forensic results.[12]

There is also a risk of the liar's dividend. Genuine evidence will be dismissed as fake when deepfakes become a significant threat. Government officials, private individuals and defendants may argue that genuine audio and video recordings have been falsified. So, the law should build authentication methods without presumptions of truth or deception. Courts should demand evidence through technical and contextual evidence, rather than viral spread or denial. This evidence discipline not only protects those harmed by deepfakes, it also protects true accountability evidence.

Evidential process remains rights-protecting. Enquiries into deepfakes involve device search, voice evidence, facial recognition, account information and platform information. These can impact on privacy and self-incrimination. Recent Supreme Court cases on bodily integrity, invasive techniques and voice samples suggest that

[11] Information Technology Act, 2000, § 69A, No. 21, Acts of Parliament, 2000 (India).
[12] Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, Gazette of India, pt. II, sec. 3(i) (Oct. 27, 2009).

investigative interests should be weighed against legality and protections. The answer is not unbridled policing, but proper orders, necessity, proportionality, data minimisation and audit logs.[13]

IX. FREE SPEECH AND THE RISKS OF OVER-REGULATION

Regulation of deepfakes inevitably affects Article 19(1)(a). A deepfake can be a lie, but it can also be art, satire, parody, political speech, visual representation of media stories, reconstruction of historical events, or even technology to assist the disabled. An outright ban on political AI, parody or synthetic media would be unlawful. Free speech in India can only be restricted under Article 19(2); and the restrictions must be reasonable. The challenge is to balance a particular evil with a specific form of speech.

Shreya Singhal provides the most obvious warning against vague internet speech laws. It declared Section 66A invalid as the words annoyance, inconvenience and gross offence were not specific grounds under Article 19(2). A deepfake law criminalising all deceptive or offensive AI-generated content might suffer a similar fate. The language of the law must be precise: non-consensual intimate synthetic media, impersonation resulting in wrongful loss, synthetic media that deceive voters about material electoral facts, child sexual abuse material, threats, extortion, and unlawful incitement. Clarity is the defence against censorship.[14]

Proportionality is also key. A restriction should be fit for the legitimate purpose, necessary to meet that purpose, and proportioned in its effect. Labelling may be less restrictive than removal for some AI-generated political or satirical content. Demonetisation should be preferred to criminal prosecution for some misleading advertisements. Removal may be appropriate for intimate deepfakes. Banning websites or accounts may only be appropriate in rare circumstances and with due process. The punishment should fit the crime.

Our freedoms also demand open government. Block and takedown orders impact on both speakers and listeners. Anuradha Bhasin highlighted the importance of review

[13] Information Technology Act, 2000, § 79, No. 21, Acts of Parliament, 2000 (India).
[14] Google India (P) Ltd. v. Visakha Industries, (2020) 4 SCC 162.

and reasoned limitations in restrictions on access to communication. With deepfakes, stealth or unreasoned takedowns can erode trust and open the door to political abuse. Even where secret investigations are necessary for criminal investigations and protection of victims, there should be review, reasons and recourse.

The constitutional balance should be reflected in a harm-based taxonomy. Category one should be inherently unlawful or deeply harmful content: child sexual abuse material, non-consensual sexual deepfakes, extortion and fraud. Category two should include context-dependent content: political deepfakes, claims affecting public order, reputation, and impersonations of public personalities. Category three should include presumptively lawful or protected speech: clearly identified satire, parody, art, research, news, and education. This does not resolve hard cases but constrains regulatory power.[15]

X. SEXUAL HARM, GENDERED VULNERABILITY, AND SOCIAL VULNERABILITY

Women, children, journalists, activists, students, and other socially vulnerable groups are the targets of many of the most damaging deepfake harms. Sexual non-consensual intimate deepfakes are an act of sexual violence even if no contact occurs. They use the victim's image or likeness to create non-consensual sexualized representation and then stigmatise them. The victim experiences humiliation, fear, damage to reputation, education or employment opportunities, and social withdrawal. The law should consider this as a dignity and autonomy harm, not just obscenity.

India's laws include provisions that could address privacy, sexually explicit material on digital media, child sexual abuse material, harassment, intimidation, and indecent representation. But this can confuse victims. Reports to police may not always be properly categorised, sites may ask for excessive evidence, and parents may discourage reporting. A victim-focused strategy should include anonymous reporting, emergent removal, counselling, evidence preservation, and deterrents

[15] MySpace Inc. v. Super Cassettes Indus. Ltd., 2016 SCC OnLine Del 6382.

against retaliatory sharing. The victim should not have to redistribute, download or view the material repeatedly just to demonstrate its existence.[16]

Children require special treatment. A digital child porn image should not be accorded less seriousness because the image is created. The social and psychological damage, risk of recirculation among offenders, and the affront to child dignity warrant a harsh response. The responsibilities of social media sites should include quick takedown, disclosure to authorities (where required), and effective algorithms to detect the reappearance of material. However, safeguards need to avoid the criminalisation of minors in situations involving peers without considering coercion, age, consent, and exploitation.

Deepfake harms can also be casted along caste, religion, region, disability or language. Deepfakes can be used to create sectarian conflict, challenge inter-faith harmony, vilify Dalit or minority activists, mock disability, or spread falsehoods in local languages that lack fact-checking facilities. The law will therefore need to focus on content regulation, along with public education on digital literacy, forensic analysis in local languages, and policing with community sensitisation. Legislation that applies only to English-speaking public figures will not be sufficient to protect India.[17]

XI. BIOMETRIC ATTRIBUTES, DATA PROTECTION AND CONSENT ARCHITECTURE

Deepfakes depend on data. A person's face, voice, walking, signature, handwriting, or dance can be used as training, prompt or cloning data. The DPDP Act is thus important, even if it doesn't explicitly use the term deepfakes everywhere. The attention it gives to personal data, lawful purpose, notice, consent, legitimate use, and obligations of data fiduciaries can be mobilised to address images, videos, and voice samples. Someone who provides a picture for one reason should not be enrolled in a synthetic-media project without knowing.

[16] Information Technology Act, 2000, §§ 67A, 67B, No. 21, Acts of Parliament, 2000 (India); Protection of Children from Sexual Offences Act, 2012, No. 32, Acts of Parliament, 2012 (India).
[17] Information Technology Act, 2000, § 67B, No. 21, Acts of Parliament, 2000 (India); Protection of Children from Sexual Offences Act, 2012, No. 32, Acts of Parliament, 2012 (India).

Consent needs to be specific. A general provision for service improvement should not permit face cloning, synthetic advertising, or public use of voice data. People are tired of consent, but this does not mean consent should be weakened. It is layered notice, prohibition of sensitive synthetic reuse without express consent, withdrawal and data fiduciary accountability. For sensitive synthetic uses of biometric or identifying data, explicit and documented consent is important.[18]

Data minimisation is also a priority. Businesses and AI service providers should only keep as much identity data as is needed. If a service features avatar creation, it should specify how long the source images will be retained, whether and how the images will be used to train the model, whether the images will be disclosed to third parties, and how users can request to have images removed. Data security is important because stolen image and voice data can be used to create deepfakes. Notification and accountability matter for deepfake prevention.

A victim may be able to use the right to erasure or correction under data protection law, but deepfakes may be distributed outside of the data fiduciary's sphere of influence. A victim may need to be removed from a platform that did not originate the deepfake, for an anonymous uploader to be traced, and for the source of the images to be held accountable. This demonstrates the need for interaction between data protection, intermediary liability, and criminal law. There is no one legal pathway.

XII. POLITICAL DEEPFAKES, ELECTIONS, AND DEMOCRATIC INTEGRITY

Political deepfakes present a special constitutional question. Free elections depend on free criticism and satire, campaigning, and debate. But they may also be misled by doctored videos or voice clones created in the lead-up to the election. A deepfake video that erroneously displays a candidate withdrawing, making community

[18] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1; Digital Personal Data Protection Act, 2023, §§ 6–7, No. 22, Acts of Parliament, 2023 (India).

comments, taking a bribe, or inciting violence, can skew voter choices before they can be rectified. The law needs to be swift, transparent and targeted.[19]

Regulation of election-related deepfakes should focus on material deceit, rather than political offensiveness. Legislation that bans all AI-political satire is unconstitutional and unworkable. Legislation prohibiting deceptive synthetic media misrepresenting a candidate, political party, election commissioner, public officer, voting process, or a material fact about an election is better. Content labelling, advertising disclaimers, take-down processes in silence periods, and platform escalation procedures can be defensible where there is actual deception of voters.

The Election Commission's voluntary and regulatory measures may be useful, but voluntary codes are insufficient when viral harm is caused by multiple platforms. A protocol should establish the need for platforms to have election-integrity escalation teams, retain reported information, respond to lawful requests in election-sensitive timeframes, and provide post-election transparency reports. But executive and partisan abuse should be avoided through reasonable orders and oversight. Regulation of deepfakes should not be abused to silence political criticism.[20]

Political deepfakes also touch on advertising. Paid promotion of synthetic impersonation should be more harshly regulated than organic satire and commentary because money can amplify deception. Companies should mandate disclosure for political ads created by AI and provide public ad libraries with sponsor, targeting (where permissible) and takedown information. India can build upon international principles of transparency, while tailoring them to Indian election laws and multiple languages.

[19] Bharatiya Sakshya Adhiniyam, 2023, No. 47, Acts of Parliament, 2023 (India).
[20] Representation of the People Act, 1951, §§ 123, 126, No. 43, Acts of Parliament, 1951 (India); Election Commission of India, Advisory to Political Parties and Social Media Platforms on Responsible Use of Artificial Intelligence in Election Campaigns (2024).

XIII. PERSONALITY RIGHTS, COMMERCIAL DEEPFAKES AND INTELLECTUAL PROPERTY

Commercial deepfakes are unauthorised uses of likeness, voice, name, performance or persona to promote products, services, sales leads, or investment opportunities. India does not have a specific personality-rights statute, but courts have recognised rights related to publicity, passing off, privacy, and impersonation. AI endorsements raise pressing concerns. Consumers could be tricked into thinking that a performer, sports star, medical practitioner, judge, teacher or government official endorses a product or a get-rich-quick scheme.[21]

IP law may help but isn't the panacea. Copyright law may protect the original work, photograph, performance, or recording of a person, but the victim of a deepfake may not necessarily be the copyright owner of the original image. Trademarks and passing off may protect goodwill or confusion in the commercial marketplace. Personality and privacy actions may be more apt to address unauthorised use of identity. It is important to recognise that the harm of a commercial deepfake is not just confusion; it is association.

There should be more responsibility for AI endorsements by advertisers and platforms. A company should not be permitted to plead ignorance if it creates synthetic content using a person's likeness without permission. Advertising platforms should have identity-verification and takedown policies for impersonation. Regulations on influencer marketing and consumer protection should also be updated to include disclosure when AI-generated people, voices or endorsements are used. People have a right to be protected from robotic charlatanism.[22]

But the law should protect parody, fan art, criticism, and other transformative works. A labelled parody may be very different from a medical scam. Factors include commercial use, risk of deceiving, permission, reputation infringement or defamation and disclosure. This test permits cultural protection while avoiding identity abuse.

[21] Ritesh Sinha v. State of Uttar Pradesh, (2019) 8 SCC 1.
[22] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.

XIV. A RIGHTS-BASED MODEL FOR INDIA

Seven principles underlie a rights-based approach to deepfakes in India. First, clarity of definition. The statute should define synthetic media, deepfake, AI-generated content, materially deceptive content, non-consensual intimate synthetic media, and synthetic impersonation. Enforcement lacks consistency without definitions. Terms should be technology-neutral to allow for new tools, yet clear enough to inform citizens, platforms, police and courts.

Second, principles concern consent and context. Synthetic use of personal identity should require consent if the use impacts dignity, privacy, commercial association or intimate autonomy. Consent should be highest with biometric and intimate expressions and more permissive with satire, research, and public interest. Principle three is the harm classification. The most severe categories should be dealt with quickly; the least public speech should be reviewed; protected speech should not be blocked.[23]

The fourth principle is fairness. All takedowns or blocks should provide reasons, logs, review, and appeal, except when confidentiality is required (temporarily) to protect victims or investigations. The fifth principle is platform accountability. Service providers should offer reporting, complaints redress, evidence retention, repeat-offender measures, and transparency reporting. They should not be imposed with vague private censorship, but neither should they side-stepped with potential harms.

The sixth principle is forensic readiness. Cyber cells, courts and regulators require technical expertise to authenticate content, detect manipulation, maintain digital evidence, and appreciate model limitations. The seventh principle is public education. The law cannot compensate for media literacy, organisational transparency and user vigilance. The public should understand that memetic videos can be faked, that voice-based appeals for help can be frauds, and that synthetic porn should be reported.[24]

[23] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.
[24] Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.

A rights-based approach should also account for differences among creators, users, platforms and users. An individual who willfully creates a non-consensual intimate deepfake should be held to higher standards than a user who unwittingly shares a video and takes it down upon request. A platform that profits from, or uses algorithms to increase, a reported deepfake should be liable for more than an infrastructure provider without editorial control. Liability should reflect knowledge, control, intent and harm.

XV. INTEGRATED DOCTRINAL SYNTHESIS

An Indian doctrine should start with two negatives. The first extreme considers deepfakes as merely technologically mediated speech and thus opposes regulation until the damage is irreparable. The second takes all deepfakes as suspicious and calls for pre-emptive censorship. Neither approach is tenable. The first undermines dignity and autonomy; the second undermines democracy. Indian constitutionalism needs a more balanced approach based on legally cognisable harms and proportionate responses.[25]

Privacy doctrine provides the moral concepts of autonomy, dignity and identity. The doctrine of free speech supplies the prohibition on vagueness, overbreadth and prior restraint. Intermediary law supplies the institutional context for the online delivery. Criminal law supplies the deterrent response to wilful and serious misuse. Privacy law supplies the ex-ante regulation of data collection, re-use and retention of the personal data used for creating deepfakes. These doctrines should not be applied in silos; deepfake cases may call for their interoperation.

The distinction between authenticity and legality should also be elicited by the courts. A fake video can be marked yet legitimate; a real video can be captured illegally or released with an ill intent; a doctored video can be illegal since it involves the violation of the identity of a person or does certain kinds of damage. Whether a video is synthetic is not the question then. The issue is, is the creation, sharing, repetition or

[25] Indecent Representation of Women (Prohibition) Act, 1986, No. 60, Acts of Parliament, 1986 (India).

profit-making of the content an infringement on consent, legally recognised damage, misleading the people, or is it an exception to freedom under Article 19(2).[26]

The regulatory design should be responsive to access to justice. A famous person can receive instant legal counsel and facebook help, but not a student, employee, or activist in the country. The law will perpetuate inequality in case deepfake solutions can be used by only the rich. The grievance system is supposed to be simple, multilingual, and available via cyber cells, platform mechanisms and victim assistance mechanisms. When handling intimate materials, privacy is paramount. The victim should not be further enhanced by the process through the compulsory procedures.

Platform economy requires responsibility. A trendy platform tactic is sensationalist clickbait. Deepfakes make use of that architecture. A platform that markets a reported impersonation video to a larger number of users, enables advertisements at a fee to synthetic scamming, or fails to take action against serial uploaders is not a neutral intermediary. Knowledge, control, dissemination and profit should be taken into consideration by the law. Safe harbour but not licence to harm should be granted to good-faith hosts.[27]

Baselines to creators of AI encompass protections against non-consensual intimate generation, voice cloning without authentication, watermarking or provenance where possible, abuse reporting, user logs (where lawful), and model constraints. Special attention must be paid to open source and scholarly research since innovation should not be smothered; however, the publication of the tools that are mainly beneficial in impersonation or sex abuse should be discussed. Design, foreseeability, safeguards and misuse after notice should be used to determine responsibility.

Policies are also needed by institutions, offices and professionals. Deepfake harassment might not be viewed as a criminal offence in the immediate future in workplaces and universities, but it can destroy careers and lives. Policies against synthetic sexual abuse, impersonation and AI harassment must be instituted in universities and workplaces. The responses of institutions must be evidenced-

[26] Protection of Children from Sexual Offences Act, 2012, No. 32, Acts of Parliament, 2012 (India).
[27] Consumer Protection Act, 2019, No. 35, Acts of Parliament, 2019 (India).

preserving and process-based. Victims do not need to be left with a choice of either being quiet or going out there.

Indian courts will play a key role in creation of remedies. Injunctions may stop distribution, secrecy orders may protect victims, damages may redress harms to dignity, and writ jurisdiction may redress non-arbitrary state action. Judge must beware when issuing global takedowns and filtering since such orders have the potential to affect legitimate speech elsewhere. Namely, evidence-based, technical orders are more apt to support rights and be effective.[28]

The final verification of deepfake regulation is to safeguard the individual without undermining the masses. Privacy is control, speech cruelty. Censorship is responsibility without due process; apathy is due process without responsibility. The law of India needs to reconcile these. It is the constitutional pledge of the rights-based approach to artificial intelligence and deepfakes.

XVI. AN INDIAN MODEL FOR INSTITUTIONALISING THE FRAMEWORK

An Indian model also has to explain how the principles can work in institutions. The first institution is the police station and the cybercrime portal. Deepfake abuse victims often require immediate help even before a court order is secured. A template for complaints should enable the victim to specify the URL (link), username, platform, date and time of discovery, alleged identity of the uploader (if known), screenshots and harm caused. Police should not consider synthetic sexual abuse as only "photo-shopped". When a complaint reveals the presence of non-consensual intimate synthetic material, identity impersonation, extortion or child sexual material, the first response should be evidence preservation and victim safety.[29]

The second institutional site is the platform complaint process. The platform should not demand the victim report the particular AI tool used. The victim may not know. The first question is whether the content appears to be a harmful image of an

[28] Tata Sons Ltd. v. Greenpeace Int'l, 2011 SCC OnLine Del 466.
[29] Int'l Covenant on Civil and Political Rights art. 17, Dec. 16, 1966, 999 U.N.T.S. 171.

identifiable person in a synthetic form and whether there is a reasonable claim of consent, fraud, threat or impersonation. The platform can do more sophisticated analysis later, but the initial response needs to stem further spread. A limited temporary restriction can avoid the irreversible if the complaint is genuine but allow restoration if it is not.

The third site is the courts. The courts will be confronted with petitions for urgent injunctions for removal, de-indexing, account data, secrecy or damages. Court orders should be specific to be executed and targeted to protect free speech. An order should name the content, harm, basis, the platforms or intermediaries, the time period and the review process. If the content is intimate or concerns children, confidentiality should be presumed. Where it is political speech, the court should avoid both confusing criticism for deception and forbidding discussion of the political matter.

The fourth institutional site is the regulator. A regulatory agency for data protection or digital services should not try to resolve all speech problems. It should establish general obligations of transparency, security, privacy, audit, grievance redressal and accountability. Decisions specifically about speech should be left to courts, legitimate government orders, election boards, or specific categories of speech covered by law. This delineation is crucial because the regulator cannot simply become an unconstrained censor of online speech.[30]

The fifth institutional site is education. Regulation of deepfakes will not be successful if the public assume everything is true until proven false or everything is false until politely convenient. Primary and secondary schools, higher education, professional associations, and campaigns should teach citizens about checking source accounts, seeking context, avoiding passing on intimate media, reporting impersonation, reverse-searching media if they can, and avoiding urgency scams. Law and literacy need to go hand in hand.

[30] Int'l Covenant on Civil and Political Rights art. 19, Dec. 16, 1966, 999 U.N.T.S. 171.

XVII. PREVENTING ABUSE OF DEEPFAKE LAW

Legislation to combat deepfakes can be abused. Political leaders can falsely assert videos are fake. Elites may argue privacy to curtail investigative journalism. Companies may over-censor legitimate content to shield themselves from risk. Law enforcement may report cases for routine criticism as doctored. These are potential abuses, following the nature of digital power. But the regulation should have safeguards at the same level as enforcement.[31]

The first is terminological rigour. The conduct should not be prohibited because it is embarrassing, offensive, or politically unpopular. The categories of prohibited content need to be tied to a harm: nonconsensual intimate depiction, child sexual material, fraud, extortion, impersonation, electoral fraud, public order incitement, or breach of privacy and data protection obligations. An offence of deceptive AI content would be too broad and would have a chilling effect on free expression.

The second safeguard is reasons. All serious takedowns, blockings and account bans should be justified, except where temporary confidentiality is needed to protect the victim. Reasons help the speaker make a decision, help the platform act on the decision, and help the court review it. They also help with institutional memory and enable policy to be based on evidence.[32]

The third safeguard is appeal. A user with removed content should be able to appeal the decision. A victim whose complaint is declined should also have a mechanism to appeal. Appeals are essential in a speech-sensitive system. They are required because deepfake systems and hasty human review can get it wrong, particularly in a multilingual, satirical, journalistic or political environment.

The fourth safety measure is public reporting. The platforms should report regularly on the number of deepfake complaints, types of action, appeal restoration, time taken to respond, government directives, and repeat offenders. Government should also publish suitable aggregate data about blocking and takedowns, with regard to victim

[31] Universal Declaration of Human Rights, G.A. Res. 217A (III), arts. 12, 19 (Dec. 10, 1948).
[32] Regulation 2022/2065, of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services, 2022 O.J. (L 277) 1.

privacy and safety concerns. This enables researchers, courts, and civil society to identify over- and under-enforcement.[33]

The fifth safeguard is proportionality of remedies. Not all breaches require criminal action. Some cases may require demonetisation, some may require removal, some may require civil damages, and some may require criminal punishment. A graduated response to wrongdoing minimises the risk of over-criminalisation and enables a more nuanced response to harm.

XVIII. FINAL NORMATIVE POSITION

The normative project of Indian regulation of deepfakes is straightforward: no individual should lose their legal or social control over the meaning of their face, voice, body or identity because their likeness can be mimicked by technology. And no one should lose the freedom to satirise, critique, experiment, or dissent simply because they use synthetic media. Dignity and democracy must be protected by law.

This is only possible with design. Consent must be meaningful. Platform duties must be real. Government power must be accountable. Criminal law must be precise. Privacy must protect the upstream use of personal data. Judges must know how to assess synthetic evidence. The populace must be taught to check before they share. A deepfake regime grounded in these principles can address the threat of AI misuse without giving up on constitutional principles.[34]

Indian law has the legal resources to create this regime. Puttaswamy gives the language of dignity and autonomy. Shreya Singhal gives the warning against vague digital speech offences. Anuradha Bhasin gives the call for reasonable restrictions and review. The DPDP Act gives the data accountability. The IT Act and IT Rules give the cyber and intermediary framework. BNS and other criminal laws give punishments for serious misuse. The challenge is to thread these into a humane law.

Deepfakes are a challenge to law's integrity, in the face of technology. A fearful legal order will over-censor. A timid legal order will leave victims unsupported. A

[33] Regulation 2024/1689, of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence, 2024 O.J. (L 1689) 1.
[34] People's Union for Civil Liberties (PUCL) v. Union of India, (1997) 1 SCC 301.

constitutional order will not. It must treat synthetic media as both a medium of speech and a medium of attack. It must criminalise malicious identity theft while enabling creative expression. It must compel platforms to be responsible, but not to police speech. It must enable the state to defend its citizens without allowing the state to become lawless. This is the key requirement for regulating artificial intelligence and deepfakes in India.[35]

XIX. SUGGESTIONS AND RECOMMENDATIONS

First, India should legislate against the non-consensual creation of intimate deepfakes. This should prohibit the creation, publication, threat of publication, and intentional distribution of non-consensual intimate deepfakes of an identifiable person. This offence should apply to all genders with accelerated civil remedies like takedown, de-indexing, privacy and damages. Intentional or reckless serious harm should attract a criminal penalty.[36]

Secondly, the IT Rules should be improved to include deepfake grievances. Companies should offer a specific avenue for complaining about synthetic impersonation, intimate deepfakes, child sexual abuse material, fraud, and election fraud. For content that is prima facie non-consensual intimate deepfakes, temporary blocking while under review may be warranted. Political and news content should be removed only in response to a lawful order, unless the content clearly breaches particular platform rules and legal criteria.

Third, labelling of AI-content should be proportional. Labels can be helpful, but excessive labelling may stifle some innocent innovation and may be impractical. The highest standards of labelling should be applied to advertisements, political speech, public-service messages, financial advice, health claims, and computer-generated impersonation. Labels should be persistent (where possible) and conspicuous and include metadata or provenance standards. Non-labelling should not be an automatic crime unless there is deception, harm, or lawbreaking.[37]

[35] Secretary, Ministry of Information & Broadcasting v. Cricket Ass'n of Bengal, (1995) 2 SCC 161.
[36] S. Rangarajan v. P. Jagjivan Ram, (1989) 2 SCC 574.
[37] Bennett Coleman & Co. v. Union of India, (1972) 2 SCC 788.

Fourthly, privacy regulations should explicitly address the use of biometric and identity-related synthetic media. AI generators collecting images, audio or video should state whether they will be stored, used, shared, or discarded. Voice cloning and face cloning should require explicit consent in reputation, commercial, political, or erotic contexts. Consent withdrawal and deletion should be easy.

Fifth, the national police should have a deepfake evidence protocol. It should contain processes for preserving URL, screenshots, hash, source, metadata, complaint statement, platform notices and chain of custody. Cyber forensic labs should standardise procedures for analysing synthetic media and provide estimates of uncertainty. And courts should be wary of claims of authenticity and claims of fraud.

Sixthly, election laws should contain a fast but reviewable mechanism for materially deceptive synthetic media in elections. The mechanism should include the Election Commission, escalation teams and reasoned orders. It should focus on deceptive imitation of candidates, election officials, polling instructions, withdrawal statements, community incitement and criminal confessions. Satire and criticism should not be censored if not misleading.[38]

Seventhly, there should be public interventions to promote digital literacy and victim empowerment. Government should release reporting guidelines in major Indian languages, encourage school and university education and establish helplines that do not stigmatise deepfake sex abuse victims. Law reform will not succeed if victims are too frightened to report or police treat synthetic sexual abuse as a trivial online prank.

XX. CONCLUSION

Deepfakes are an issue in India as they border on free speech, identity, privacy, evidence, fraud, and political persuasion. They are not some sort of fake news. They are techno-acts that are able to rob an individual the face, voice, body and reputation as they pass through the media at viral speed. Indian law must not be censorious in the response but must be grave. The Constitution requires the style which will protect

[38] Indian Express Newspapers (Bombay) (P) Ltd. v. Union of India, (1985) 1 SCC 641.

the dignity without straining out dissent; will regulate platforms without delegating the censorship; and will penalize maltreatment without criminalizing art.[39]

We have very substantial materials in our current legal structure. The IT Act provides provisions of cyber-law; the IT Rules provides provisions of intermediary due diligence; the DPDP Act provides provisions of data protection; the Bharatiya Nyaya Sanhita criminalises harms; Puttaswamy constitutionalises privacy and Shreya Singhal prevents vague censorship on online speech. The question is how to transform these materials into a deepfake system. We must swap disintegration with clarity, consideration of the victim and sensible platform requirements, forensic skills and responsible state behavior.

The best regulatory practice in India is a multi-faceted one. Unauthorized sexual deepfakes, child porn deep fakes, fraud, extortion and impersonation should be dealt with. Only legal procedures should be used to review, tag and remove political and public-interest speech. Deepfakes in the business world require permission, openness and legalization of consumers. The privacy guarantees are needed in data-driven tools, security requirements and limitations on identity reuse. This method takes into account the advantages and disadvantages of artificial intelligence.[40]

The greater problem is credibility. The legislation is not able to regain the confidence on the digital media by banning any synthetic images. It can, however, be able to blame those who abuse the synthetic media and bring harm to the dignity, democracy and security. It can guarantee that there are no victims left alone, platforms are not lazy and the government is not overstepping. A constitutionally grounded Indian deepfake regime must, therefore, be based on legality, proportionality, transparency, consent and remedy. It is one means of controlling AI without sacrificing privacy, speech and democracy.

[39] D.M. Ent. Pvt. Ltd. v. Baby Gift House, 2010 SCC OnLine Del 4790.
[40] Titan Indus. Ltd. v. Ramkumar Jewellers, 2012 SCC OnLine Del 2382.

XXI. REFERENCES

A. Statutes and Legislative Materials

1. Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023 (India).
2. Bharatiya Sakshya Adhiniyam, 2023, No. 47, Acts of Parliament, 2023 (India).
3. Consumer Protection Act, 2019, No. 35, Acts of Parliament, 2019 (India).
4. Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
5. Indecent Representation of Women (Prohibition) Act, 1986, No. 60, Acts of Parliament, 1986 (India).
6. Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
7. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Gazette of India, pt. II, sec. 3(i) (25 February 2021).
8. Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, Gazette of India, pt. II, sec. 3(i) (27 October 2009).
9. Protection of Children from Sexual Offences Act, 2012, No. 32, Acts of Parliament, 2012 (India).
10. Representation of the People Act, 1951, No. 43, Acts of Parliament, 1951 (India).

B. Government and Regulatory Materials

1. Election Commission of India, *Advisory to Political Parties and Social Media Platforms on Responsible Use of Artificial Intelligence in Election Campaigns* (2024).
2. Ministry of Electronics and Information Technology, Government of India, *Advisory on Compliance with the Information Technology (Intermediary*

Guidelines and Digital Media Ethics Code) Rules, 2021 in Relation to Deepfakes and AI-Generated Content (November 2023).

3. Ministry of Electronics and Information Technology, Government of India, *Further Advisory on Intermediary Obligations Concerning Deepfakes and Synthetic Media* (December 2023).

C. Cases

1. *Amitabh Bachchan v Rajat Nagi & Ors*, CS(COMM) 819/2022 (Delhi High Court).
2. *Anil Kapoor v Simply Life India & Ors*, CS(COMM) 652/2023 (Delhi High Court).
3. *Anuradha Bhasin v Union of India* (2020) 3 SCC 637.
4. *Anvar P.V. v P.K. Basheer* (2014) 10 SCC 473.
5. *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal* (2020) 7 SCC 1.
6. *Bennett Coleman & Co. v Union of India* (1972) 2 SCC 788.
7. *Christian Louboutin SAS v Nakul Bajaj* 2018 SCC OnLine Del 12215.
8. *D.M. Entertainment Pvt. Ltd. v Baby Gift House* 2010 SCC OnLine Del 4790.
9. *Google India (P) Ltd. v Visakha Industries* (2020) 4 SCC 162.
10. *Indian Express Newspapers (Bombay) (P) Ltd. v Union of India* (1985) 1 SCC 641.
11. *Jackie Shroff v The Peppy Store & Ors*, CS(COMM) 590/2024 (Delhi High Court).
12. *Justice K.S. Puttaswamy (Retd.) v Union of India* (2017) 10 SCC 1.
13. *MySpace Inc. v Super Cassettes Industries Ltd.* 2016 SCC OnLine Del 6382.
14. *People's Union for Civil Liberties (PUCL) v Union of India* (1997) 1 SCC 301.
15. *R. Rajagopal v State of Tamil Nadu* (1994) 6 SCC 632.
16. *Ritesh Sinha v State of Uttar Pradesh* (2019) 8 SCC 1.
17. *S. Rangarajan v P. Jagjivan Ram* (1989) 2 SCC 574.

18. *Secretary, Ministry of Information and Broadcasting v Cricket Association of Bengal* (1995) 2 SCC 161.

19. *Selvi v State of Karnataka* (2010) 7 SCC 263.

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

21. *Swami Ramdev v Facebook, Inc.* 2019 SCC OnLine Del 10701.

22. *Tata Sons Ltd. v Greenpeace International* 2011 SCC OnLine Del 466.

23. *Titan Industries Ltd. v Ramkumar Jewellers* 2012 SCC OnLine Del 2382.

D. International Instruments

1. International Covenant on Civil and Political Rights, 16 December 1966, 999 UNTS 171.

2. Universal Declaration of Human Rights, GA Res 217A (III), UN Doc A/810 (10 December 1948).

E. European Union Instruments

1. 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] OJ L 277/1.

2. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) [2024] OJ L 1689/1.