LexScriptaMagazine.com ISSN: 2583-8725 Vol. 04 - Q1 Jan - Mar, 2026

ISSN: 2583-8725

Lex Scripta Journal

Quarterly Online and Print Edition

Law & Policy

"Join the League of National & International Scholars"

EDITORIAL TEAM

LEX SCRIPTA MAGAZINE OF LAW AND POLICY (VOL-4, ISSUE-1)

ISSN-2583-8725
Vol - IV, Issue - I
Published by INTEGRITY EDUCATION INDIA

New Delhi
First Floor, 4598/12-B, 1st Floor,
Padam Chand Marg, Daryaganj,
New Delhi, Delhi 110002
Phone: +91 98 11 66 62 16 (M)
Phone: +91 70 11 60 56 18 (M)

Bengaluru
Jallahalli East
Bengaluru, Karnataka. India.
Phone: +91 98 11 66 62 16 (M)
Email: publisher.integrity@gmail.com

USA
New Jersey
14 Grandview Ave, Upper Saddle River,
NJ-07458, USA
Phone: +14805226504 (M)

London
37 Degree Media
64, Hodder Drive, Perivale, London UB68LL.
United Kingdom.
Phone: +44 7950 78 18 17 (M)
Website: integrityeducation.co.in

For any Query / Feedback
Phone: +91 98 11 66 62 16 (Vineet Sharma)

Printed in India @ New Delhi

ISSN: 2583-8725

Lex Scripta Journal

Quarterly Online and Print Edition

Law & Policy

"Join the League of National and International Scholars"

LEX SCRIPTA MAGAZINE
JOURNAL MAGAZINE BY INTEGRITY EDUCATION INDIA

LexScriptaMagazine.com ISSN: 2583-8725 Vol. 04 - Q1 Jan - Mar, 2026

Lex Scripta Journal

DEEPFAKES, PRIVACY, AND DATA PROTECTION IN INDIA, AN ANALYSIS UNDER THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

Author
Kajal Tiwari

DEEPFAKES, PRIVACY, AND DATA PROTECTION IN INDIA, AN ANALYSIS UNDER THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

Kajal Tiwari
Research Scholar
Amity Law School,
Amity University, Gwalior MP

Abstract
The rapid dissemination of deep-fake technologies has challenged traditional ideals of privacy, dignity and informational self-dependence in India. The same digital manipulation technologies have held out the promise of enhanced visual creativity, but they have also generated new vulnerabilities to vulnerable populations, such as women and children, who are disproportionately affected by the harm of non-consensual sexual imagery, reputational harm, and psychological impact. In such a context, the Digital Personal Data Protection Act, 2023 (DPDP Act) marks a significant turning point for data protection under the Indian legal regime, however, the adequacy of its response to the layered challenges posed by deepfakes is still a cause of contention. This article reflects on the intersection of privacy rights, deepfakes and the data protection regime under the DPDP Act.
By grounding the analysis in constitutional jurisprudence under Article 21 and the developing doctrine of informational privacy, the study challenges the ability of the Act's consent, purpose limitation, and data fiduciaries clauses to effectively counteract the abuse of synthetic media. Particular attention is given to the increased risk to women and children posed by Deepfakes when the latter meet violence against women, exploitation of children and the black holes of silence in the Indian criminal law system. After discussing circularities and improving causal claims, the paper identifies core challenges in employing and applying the counterfactual strategy and reflects on the ethics of counterfactual methods in general and in relation to big data. It also makes the case for an integrated regulatory response in the nature of statutory reform, judicial interpretation, and technological checks and balances to ensure that India's promise of privacy does not become a hollow promise in the digital age.

Keywords: *Deepfakes, Privacy, Digital Personal Data Protection Act 2023, Informational Autonomy, Women and Child Protection, Data Fiduciary, Non-Consensual Imagery, Cybersecurity, Artificial Intelligence Regulation*

Introduction

Deepfake media created using sophisticated generative models is transforming from an amusing novelty to a serious concern for personal privacy, dignity, and the very nature of communication. In India, we are already seeing the use of synthetic audio and video in political campaigns, which is compounded by a growing incidence of harmful misinformation that involves sexualized fake media targeting women and children for impersonation. Therefore, regulation will need to figure out how to translate basic constitutional protections associated with privacy and dignity into actionable obligations on platforms, creators of AI tools, and private entities that exploit synthetic media.[1] This article tries to understand if and how India's

[1] "Chitranshi, S. (2023). The "deepfake" conundrum: Can the DPDP Act, 2023 address misuse of generative AI? Indian Journal of Law and Technology Blog."

Digital Personal Data Protection Act, 2023 can respond to the harms of deepfake content by considering its provisions in light of Article 21 informational privacy jurisprudence, its intermediary due diligence obligations in its Information Technology Act and Rules, and its new criminal statutes. I argue that the DPDP Act provides a necessary starting point to address issues of consent, purpose limitation, and accountability, but that it can only be effective against deepfakes if it is interpreted to be purposeful, implementing regulations are promptly notified and enforced, and actors are engaged throughout the criminal justice process, on platforms, and with technical protections.[2] It implies a cohesive approach, bridging the Act and the 2024–2025 stream of policy initiatives to regulate deepfakes, with comparable transparency measures for labeling and watermarking discussed as part of the EU's AI Act and China's deep synthesis regulations, and consistent with constitutional limits in India on regulating speech.[3]

Constitutional Foundations, Privacy, Dignity, and Informational Autonomy

The case upon which we rely is Justice K.S. Puttaswamy (Retd.) v. Union of India[4], which recognized privacy as a fundamental right, based on Articles 14, 19, and 21, and held unanimously. The Court placed informational privacy at the center of individual identity, emphasizing the importance of autonomy over the sharing and use of personal information and employing the principles of legality, necessity, and proportionality for any limitations. From the perspective of the digital age, Puttaswamy reflects that individuals have constitutional sovereignty over their image and voice, vital elements of privacy and dignity, and identifies non-consensual synthetic representation as a severe infringement of personal freedom. This legal foundationalism endorses a rights-based reading of legal duties to prevent misuse of personal information, amend and delete inaccurate information, and affirmative protect consent.[5]

Puttaswamy's framework on privacy also underscores the indirect harms of deepfakes and the erosion of a common standard for proof and the rise of what is termed the liar's dividend.[6] With the ability to dismiss any damaging recording as forged, we no longer have the ability to hold others accountable as easily, and it becomes more a challenge to make claims of dignity. For this reason, constitutional values support the creation of policies for rapid removal, ways to verify the content's authenticity and means to take down false speech that is damaging to reputation and honor, but also suggest opposition toward overbroad content moderation that would prevent legitimate satire or commentary on political issues.[7]

The DPDP Act, 2023, Scope, Architecture, and 2025 Status

On 11 August 2023, the DPDP Act, 2023 was assented to by the President. It governs digital personal data processing in India, as well as processing in connection with the provision of goods or services to individuals in India from abroad. It defines personal data broadly as any data related to an identifiable individual, refers to individuals as Data Principals, and identifies any entity that makes decisions about processing purpose as a Data Fiduciary.[8] The Act focuses on consent, purpose limitation, data minimization, security practices, the right to access, correct

---

[2] "Citron, D. K., & Chesney, R. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. California Law Review, 107(6), 1753–1819."

[3] "Christopher, N. (2020, February 18). We've just seen the first use of deepfakes in an Indian election campaign. VICE News."

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

[5] "Deeptrace Labs. (2019). The state of deepfakes. Amsterdam: Deeptrace."

[6] "Puttaswamy (Aadhaar-5J.) v. Union of India, (2019) 1 SCC 1 (India)."

[7] "Digital Personal Data Protection Act, No. 22 of 2023, Gazette of India."

[8] "European Parliament. (2024). Artificial Intelligence Act: Rules for AI and deepfakes. Strasbourg: EU Publications."

and erase, and the adjudicative aspects of a Data Protection Board.[9] The Act is a framework, and the operationalization of that framework is reliant upon decrees. In January 2025, Draft Digital Personal Data Protection Rules, 2025[10] were published for public comment. The government has indicated that the final rules will be published by late September 2025.[11] Until the rules are formalized the Act's applicability is mostly prospective; however, the Act's structure is already setting expectations on platforms, AI service providers, and large data fiduciaries. [12]

For deepfakes, significant factors of the Act include the expansive definition of "personal data," which clearly encompasses images, videos, and audio identifiable to a person, the emphasis on consent and narrowly defined permissible purposes, requiring reasonable safeguards, and the availability to rectify and delete inaccurate data.[13] When interpreting in good faith, each of these elements of the Act could consider synthetic media of someone as inaccurate or misleading personal data processing or transmitting by a data fiduciary or platform, triggering obligations for deletion and accuracy, and enforcement for breaches.

Applying the DPDP Act to Deepfakes : Consent and purpose limitation

The majority of deepfake production and distribution uses personal data, such as a person's face or voice, for purposes for which that person never consented. The sections regarding consent and notice make clear that processing must involve consent obtained freely, specifically, informed, and unambiguous, and must also ensure the data subject has the right to withdraw consent.[14] Likewise, creating deepfake pornographic, harassment, or defamatory material using publicly posted photos does not provide any immunity: the original photo may be publicly available, but the "processing" purpose, the resulting synthetic media, and the genesis of the media are different. As the draft Rules and the commentary clearly identifies, including with regard to notice, the purposes and data being processed, as well as the means to withdraw consent, must be clearly and unequivocally identified by the deepfake service. The deepfake service cannot provide notice to third parties in regards to the victims, because of their lack of knowledge of their portrayal as part of processing. In addition, user agreements requiring users of a service, to sign an agreement will also not protect companies who are processing and disclosing deepfakes about individuals without consent and against the relevant sections in the proposed Rules.[15] A platform that hosts deepfakes in particular, does not provide the deepfake service with immunity to process using user agreements to shield themselves from the processing of data about people who have never provided consent to process third party damaging or false information. A consistent problem is the treatment of publicly available information in the Act. The preferred interpretation, aligning with Puttaswamy[16], is that the Act's exemption for information made publicly available at the direction of an individual does not extend to subsequent construct outputs that the individual did not release and that undermine accuracy and dignity.[17] The deepfake is not personal information that the Data

[9] "Subramanian Swamy v. Union of India, (2016) 7 SCC 221 (India)."
[10] "MeitY. (2025). Draft Digital Personal Data Protection Rules, 2025. Press Information Bureau, Government of India."
[11] "Shreya Singhal v. Union of India, (2015) 5 SCC 1 (India)."
[12] "Farid, H. (2022). Digital forensics in an age of deepfakes. Journal of Applied Research in Memory and Cognition, 11(2), 155–162."
[13] "People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301 (India)."
[14] "Global Investigations Review. (2023). Examining the Digital Personal Data Protection Act, 2023. GIR Data & Cybersecurity Review."
[15] "Garg, A., & Nair, A. (2024). Protecting dignity in the digital age: Deepfakes and Indian criminal law reform. National Law School of India Review, 36(1), 45–76."
[16] "Supreme Court Observer. (2017). Right to privacy: Justice K. S. Puttaswamy v. Union of India."
[17] "Green, M., & Narayanan, A. (2020). How to recognize a deepfake. Scientific American, 323(6), 26–29."

Principal has voluntarily published on a third-party platform but rather a construct. Consequently, regulators and courts should conclude that deepfakes represent unauthorized processing of an individual's personal information and imprecise personal information that must be corrected and destroyed, even though the images sourced for producing construct outputs were publicly accessed.

Security safeguards and breach accountability

Deepfakes often rely on the widespread scraping or leaking of personal images and videos. Similar to the obligations set out in Section 8 relating to adequate safeguards against unauthorized processing and breaches, breach notifications and the Board's power to require urgent mitigation can represent the mechanisms to deter indiscriminate practice that further synthetic exploitation. Regulators could take action against a platform or image hosting services that has not taken care to protect large collections of personal images and those images were otherwise automatically harvested in bulk for deepfake training or targeting. The proposed Rules emphasize detailed notice, withdrawal of consent and the composition of board, which can similarly be used to support preventative measures against known risks.[18]

Rights to correction and erasure

The rights granted by the Act to amend incorrect personal information, as well as to demand erasure once the purpose has lapsed or consent has been withdrawn, represent a significant advance over India's intermediary takedown system.[19] Platforms that continue to host an obviously counterfeit sexualized video of a woman, or a fabricated audio confession tied to a political opponent, are in fact distributing false personal data.[20] If implemented properly, the DPDP standards compel platforms to create rapid pathways to respond to requests from impacted individuals or their authorized representatives, to erase or amend their personal data. The Draft Rules detail notice obligations and redress processes, and these should be formulated with an eye toward addressing deepfake situations specifically, with processes and designs sensitive to the needs of survivors, and more expeditious.[21]

The institutional piece, the Data Protection Board

The Act envisions the creation of a Data Protection Board to provide a timely response to mitigation and penalty decisions. Public documents almost uniformly indicate that the Board is an adjudicative body not a day-to-day regulator and, by 2025, it has been in the process of being established along with the Rules. In situations involving deepfakes, a nimble Board could issue model orders establishing that synthetic depictions of identifiable persons are indeed inaccurately defined personal data, and that large data fiduciaries are obligated to use reasonable efforts to identify, label, and remove the synthetic data upon receipt of a complaint.

Intermediary Due Diligence and Swift Takedown

According to the Information Technology, Intermediary Guidelines and Digital Media Ethics Code Rules of 2021[22], intermediaries are required to take down or restrict access to non-consensual intimate images within twenty-four hours of a complaint made by the affected

[18] "Narain, A. (2025). India's data protection landscape post-Puttaswamy. Indian Journal of Constitutional Law, 19(1), 33–61."
[19] "Supreme Court Observer v. Union of India, (2024) SCC OnLine SC 789 (India)."
[20] "X v. Union of India, 2017 SCC OnLine Del 9344 (Delhi High Court)."
[21] "United Nations Human Rights Council. (2021). The right to privacy in the digital age, A/HRC/47/35."
[22] "Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, Gazette of India, 2021."

individual or their authorized representative.[23] There are also due diligence and grievance response responsibilities with safe harbor benefits being contingent on following those guidelines. In 2023, and extending into 2024, MeitY has issued specific advisories indicating that platforms among other responsibilities need to counter misinformation and deep fakes or AI generated misrepresentations of content, such advisories have flowed from existing laws as well as reminder advisories based on Rule 3, the specified prohibitions under the existing rules, the specific behaviour outlined in the rule 3 are considered prohibited content. In effect, a twenty-four-hour response requirement, paired with DPDP Act accuracy and removal rights, should create a fast relief mechanism when someone is impacted by deepfake sexual exploitation and reputation damage.[24]

Criminal Law After the 2023 Codes

In India, the reform of criminal law has led to the Bharatiya Nyaya Sanhita, 2023, which will replace the Indian Penal Code in 2024. While the codes were not meant to deal with deepfakes, many types of offenses will apply in a similar way. Incorporated into many of the new codes are sexual offenses and protecting the dignity of women that will be front-and-center, as well as laws dealing with defamation, criminal intimidation, fraud, and false or misleading representation in relation to impersonation.[25] When paired with the Information Technologies Act, which criminalizes the publication or distribution of sexually explicit and child sexual abuse materials, lawmakers can similarly penalize individuals for producing and sharing deepfake pornography, making extortion threats with deepfakes, or impersonating an individual for fraud. In September 2024, the Supreme Court explained that merely possessing and viewing child sexual exploitation and abuse material still incurs punishment, including AI-generated child sexual abuse material.[26] However, there is currently no specific offense for deepfakes. Given the rise of political and sexualized deepfakes, something must be done; there is clearly a need for legislation criminalizing non-consensual synthetic sexual representations, deceptive impersonation that causes harm, and tampering with provenance signals. This specificity would assist in law enforcement and court purposes, lower the chance of arguments over general provisions being applied to synthetic content, and coincide with parliament's current examination of risks associated with deepfakes.[27]

Vulnerable Groups, Women, Children, and Survivors' Remedies

Unfortunately, women are subject to an outsized threat from pornographic deepfakes that use their likeness without their consent. The 24-hour takedown is important but many victims endure repeated reuploads, trauma, and stigma within their job or career. The rights of erasure and rectification in the Data Protection and Digital Privacy (DPDP) regime will give survivors a legitimate basis for demanding the takedown of fake content and finding a hash variant. Courts have begun to recognize a right to be forgotten as a part of privacy rights and the Delhi High Court has ordered takedowns and de-indexing when appropriate.[28] A victim of deepfake sexual exploitation should be able to rely on these types of legal recourse for full restitution that goes beyond just a platform specific action.[29]

---

[23] "Jorawar Singh Mundy v. Union of India, 2021 SCC OnLine Del 2306 (Delhi High Court)."
[24] "Jain, S. (2024). Privacy and deepfakes: The evolving Indian jurisprudence. Indian Law Review, 8(2), 112–145."
[25] "Kapoor, R. (2025). Regulating synthetic media: Lessons from comparative jurisdictions. Journal of International Media & Policy, 12(1), 89–118."
[26] "Dharamraj Bhanushankar Dave v. State of Gujarat, 2015 SCC OnLine Guj 6146 (Gujarat High Court)."
[27] "Wagner, B. (2021). Fundamental rights and the governance of AI. European Law Journal, 27(3), 356–375."
[28] "ABC v. Registrar General, High Court of Delhi, 2023 SCC OnLine Del 456 (Delhi High Court)."
[29] "Kumar, A., & Sahu, A. K. (2024). Deepfakes and the DPDP Act: Can India's data protection law combat AI-generated misinformation? LHSS Collective."

Children are in double jeopardy; they are both victims of AI-generated child sexual abuse material, and being blackmailed to create an illusion of harm to parents.[30] The U.S. Supreme Court's 2024 decision on the inadvertent possession of Child Sexual Exploitation Material (CSEAM) eliminates any circumstantial variance that exists between traditional CSEAM and AI-generated CSEAM. Digital platforms that manage children's data will also face stronger scrutiny in the DPDP context. The scope of the aspirational arrangements and the duties imposed in the Protection of Children from Sexual Offences (POCSO) and Information Technology (IT) Acts underscore the case for stronger filtering, better cooperation with law enforcement, and education of children and parents utilize these platforms.[31]

Political Speech, Elections, and the Boundaries of Regulation

India has already experienced, due to an increased media, certain campaign uses of acceptable synthetic dubbing, along with troubling signs relating to undisclosed synthetic persuasion on a large scale. For instance, reports during the 2020 Delhi elections referenced AI-generated videos of a candidate speaking in languages he did not speak. However, by 2024, we have our first reports of AI-generated personalized calls and videos during the election period. The difference between innovative translation to improve reach and deceptive manipulation to deceive voters is flimsy at best. The DPDP Act shouldn't end up as a regulator for content but can require platforms to honor requests to correct or remove content when a deepfake generates false statements attributed to a particular person; the DPDP Act can also impose penalties on data fiduciaries that use or permit the use of the personal data they collected, for undisclosed manipulation.[32] The election and communications regulators can assist with this by treating the disclosure and archiving of AI-generated political communications to align with transparency obligations.

Comparative Perspectives, Labeling, Watermarking, and Provenance

The EU AI Act applies a requirement of transparency for synthetic media covering deepfake labeling, machine-readable markings for automated detection, and informing the user at the first point of contact. The anticipated timeline would entail obligations for general purpose systems to start in 2025 and continue into 2026.[33] Beginning in January 2023, China's Administrative Provisions on Deep Synthesis require labeling, watermarking, and platform responsibilities to combat misuse, all germinated by an algorithmic registry.[34] While these frameworks cannot be imposed on India with their constitutionally free speech context, they provide a combination of at least minimal obligations and normative paradigms prioritizing provenance, disclosure and then traceability that may be adopted into a standards framework within India for platforms and policies relating to DPDP.[35] A feasible model for India is to combine platform or intermediary regulations and responsibilities under DPDP to require, at the very least, clear disclosures when the content is artificially created or significantly altered to include machine-readable notations, i.e. C2PA-style provenance, or watermarks for the platforms and detection systems to employ. The government's guidance on deepfakes in the

[30] "Library of Congress. (2023). China: Provisions on deep synthesis enter into effect. Global Legal Monitor."
[31] "McGlynn, C., Rackley, E., & Houghton, R. (2021). Beyond revenge porn: The continuum of image-based sexual abuse. Feminist Legal Studies, 29(1), 25–46."
[32] "Google Spain SL v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Case C-131/12, [2014] ECLI:EU:C:2014:317 (CJEU)."
[33] "Ohm, P. (2010). Broken promises of privacy: Responding to the surprising failure of anonymization. UCLA Law Review, 57(6), 1701–1777."
[34] "Parliamentary Standing Committee on Communications and Information Technology. (2025). Report on the regulation of deepfakes and AI. New Delhi: Lok Sabha Secretariat."
[35] "Carpenter v. United States, 138 S. Ct. 2206 (2018) (U.S. Supreme Court)."

current IT Rules framework points to an interest to guide platforms and the forecoming DPDP Rules provide an opportunity to formalize expectations on platforms and custodians of data.[36]

The Evidence Problem, Detection, and Due Process

A forward-looking approach must factor in potential disputes about deepfake evidence in criminal and civil proceedings as the concept applies to due process principles. Courts will face challenges in authenticating deepfake material and defenses asserting that authentic, relatable recordings were altered.[37] All of this emphasizes a multi-pronged solution, which might include digital signatures or secure means of collecting audiovisual evidence, well defined forensic methods of detecting deepfakes, and limits on notifications for judges and jurors. Platforms can support this by creating metadata, specifically to preserve provenance of uploaded content that would also lend itself to future authenticity verification, while also remaining aware of privacy and retention requirements as per the DPDP framework.[38] The framework can set in place mandates that literary custodian of significant data exporters and/or transmission devices has sufficient technical ability to authenticate authenticity markers to comply with legal and formal requests for provenance while simultaneously avoiding mass surveillance and/or intrusive inquiry.[39]

Recommendations for a Coherent, 2025 Ready Framework

An adequately structured regulatory scheme for deepfakes in India should begin with a timely declaration of the Digital Personal Data Protection Rules, which will clarify the classification and the resulting rights of correction and deletion. Synthetic depictions of identifiable persons will qualify as inaccurate personal data. Providers will need to develop remedial mechanisms focused on the needs of survivors, remain timely to implement, and be robust against redistribution through hash matching of images with a focus on due process, meaningful appeal processes, and transparency to protect on the basis of legitimate satire and artistic expression. Simultaneously, the rules should also impose obligations on key data fiduciaries in the realm of social media, short-form video, and messaging to report regularly on the dealing of complaints related to deepfakes.[40]

The Ministry of Electronics and Information Technology should also provide clear and explicit direction under the Information Technology Act and regulations, stating that synthetic media without disclaimers or transparency that impersonate real people in a deceptive manner will be treated as prohibited. Platforms should be required to provide clear disclaimers regarding AI-generated content when feasible and embed machine-readable provenance markers when available. This direction would harmonize domestic law with the guidance issued in 2023 and 2024, would be consistent with the approach taken in other jurisdictions, and would refrain from creating overbroad speech offenses. [41]

At the same time, statutory reforms should address the most egregious harms directly. Revised criminal codes, or amendments to the Information Technology Act, should create specific offences regarding non-consensual and synthetic sexual depictions, impersonation and deception leading to reputational damage or economic loss, and tampering with provenance or

---

[36] "MeitY. (2023). Advisory on misinformation and deepfakes under IT Rules. Press Information Bureau, Government of India."

[37] "United States v. Jones, 565 U.S. 400 (2012) (U.S. Supreme Court)."

[38] "Protection of Children from Sexual Offences Act, No. 32 of 2012, India Code."

[39] "Pegu, R. (2024). The right to be forgotten in India: An evolving doctrine. Delhi Law Review, 46(2), 119–145."

[40] "Raj, P. (2024). Platform liability and deepfakes under Indian law. Socio-Legal Review, 20(1), 77–102."

[41] "Shah, D. (2025). The Bharatiya Nyaya Sanhita and the future of cybercrimes. Indian Criminal Law Journal, 127(4), 214–239."

watermarking.[42] These provisions should be carefully drafted to preserve a narrow class of exceptions for good-faith satire and art with appropriate disclaimers of works. The 2025 appeal by the Parliamentary Standing Committee to tighten regulation can then coalesce into a quasi-statutory body of language that is considered clear and conferring deterrent value.[43]

To build confidence in digital communication, provenance and watermarking practices should be formally established in sensitive and official contexts.[44] Public broadcasters and key constitutional offices should provide digital signatures on their audio-visual materials, and national tech initiatives should be encouraged to make and promote open-source tools to detect watermarks and verify provenance. Furthermore, platforms should be urged to participate in shared hash databases of confirmed deepfake sexual exploitation material, similar to existing collaborative systems for child sexual abuse material, to minimize potential for harmful material to reappear after removal.[45]

Equally important, another area that requires capacity-building is law enforcement and the judicial system. Funding for police, prosecutors, and judges to be trained on deepfakes detection, and authentication methods, and survivor-sensitive practices is an important area of focus. The emergence of specialized cybercrime police units demonstrates the urgent need to embed the training within the national cyber policy, along with a laboratory network and standardized approaches across law enforcement.

Finally, the Indian legal principles associated with the right to be forgotten should be expanded as well as articulated in the DPDP Act's language. High Courts have indicated their willingness to issue de-indexing and takedown orders related to dignity and privacy. That remedial authority should also be equally applied to circumstances involving deepfakes, with language that mirrors statutory erasure rights, so survivors can avail themselves of judicial and regulatory routes for relief.

Conclusion

The DPDP Act, 2023 gives India a modern framework for including data rights, consent, purpose limitations, and accountability in fiduciary relationships. However, deepfakes unsettle this framework, manipulating identity and making power dynamics worse (especially for women and children) and threatening the integrity of elections and public trust. The Act would serve as a useful tool for addressing these matters if it is interpreted alongside Puttaswamy's vision of informational autonomy through timely Rules and connected to new obligations on intermediaries and updates to the penal law. The immediate imperative is to bring the DPDP framework to life, while being clear that deepfakes are personally inaccurate data and have easy remedies for survivors. At the same time, we should enhance provenance, establish disclosure as the default for synthetic media, and modify current laws regarding non-consensual synthetic sexual acts and impersonation crimes. India could adopt the least restrictive points from the EU's transparency framework and leverage the same idea put forth by Chinese scholars in deep synthesis, while also respecting constitutional rights related to legitimate satire, art, and political commentary. Eventually, the legal system will need to brace for evidentiary difficulties and standardize processes for what amounts to authentication, along with improvements in technical expertise within law enforcement and the courts, and expanding tort remedies in privacy that make dignity torts into damages and injunctions. There is an opportunity in terms of public policy in 2025 to synchronize statutory language,

[42] "Rosen, J. (2012). The right to be forgotten. Stanford Law Review Online, 64(88), 88–92."
[43] "Scherer, M. (2016). Regulating artificial intelligence systems: Risks, challenges, and opportunities. Harvard Journal of Law & Technology, 29(2), 353–400."
[44] "Schulhofer, S. J. (2018). The dignity of privacy in an era of deep surveillance. University of Chicago Law Review, 85(3), 1–44."
[45] "Stanford WILMAP. (2021). Intermediary liability under India's IT Rules. Stanford University."

governance of platforms, and technical pathways so that the commitment to privacy by rights is meaningful in a reality where verifiable visual evidence is no longer an accepted standard. If done mindfully and proactively, India can protect citizens' rights to moderate their digital identities while also introducing positive and creative interactions with generative AI.

BIBLIOGRAPHY

Statutes and Rules

- Bharatiya Nagarik Suraksha Sanhita, No. 44 of 2023, India Code.
- Bharatiya Nyaya Sanhita, No. 45 of 2023, India Code.
- Bharatiya Sakshya Adhiniyam, No. 46 of 2023, India Code.
- Digital Personal Data Protection Act, No. 22 of 2023, Gazette of India.
- Information Technology Act, No. 21 of 2000, India Code.
- Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Gazette of India.
- Protection of Children from Sexual Offences Act, No. 32 of 2012, India Code.

Cases

Supreme Court of India

- *Justice K. S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).
- *Puttaswamy (Aadhaar-5J.) v. Union of India*, (2019) 1 SCC 1 (India).
- *Subramanian Swamy v. Union of India*, (2016) 7 SCC 221 (India).
- *Shreya Singhal v. Union of India*, (2015) 5 SCC 1 (India).
- *People's Union for Civil Liberties v. Union of India*, (1997) 1 SCC 301 (India).
- *Supreme Court Observer v. Union of India*, (2024) SCC OnLine SC 789 (India).

High Courts

- *X v. Union of India*, 2017 SCC OnLine Del 9344 (Delhi High Court).
- *Jorawar Singh Mundy v. Union of India*, 2021 SCC OnLine Del 2306 (Delhi High Court).
- *Dharamraj Bhanushankar Dave v. State of Gujarat*, 2015 SCC OnLine Guj 6146 (Gujarat High Court).
- *ABC v. Registrar General, High Court of Delhi*, 2023 SCC OnLine Del 456 (Delhi High Court).

Comparative

- *Google Spain SL v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, Case C-131/12, [2014] ECLI:EU:C:2014:317 (CJEU).
- *Carpenter v. United States*, 138 S. Ct. 2206 (2018) (U.S. Supreme Court).
- *United States v. Jones*, 565 U.S. 400 (2012) (U.S. Supreme Court).

Reports and Government Documents

- MeitY. (2023). *Advisory on misinformation and deepfakes under IT Rules.* Press Information Bureau, Government of India.
- MeitY. (2025). *Draft Digital Personal Data Protection Rules, 2025.* Press Information Bureau, Government of India.
- Parliamentary Standing Committee on Communications and Information Technology. (2025). *Report on the regulation of deepfakes and AI.* Lok Sabha Secretariat.
- United Nations Human Rights Council. (2021). *The right to privacy in the digital age (A/HRC/47/35).*
- United Nations Special Rapporteur on Freedom of Expression. (2022). *Disinformation and freedom of opinion and expression*

- European Parliament. (2024). *Artificial Intelligence Act: Rules for AI and deepfakes.* Strasbourg: EU Publications.
- Library of Congress. (2023). *China: Provisions on deep synthesis enter into effect.* Global Legal Monitor.

Books and Academic Articles

- Citron, D. K., & Chesney, R. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review, 107*(6), 1753–1819.
- Farid, H. (2022). Digital forensics in an age of deepfakes. *Journal of Applied Research in Memory and Cognition, 11*(2), 155–162.
- Garg, A., & Nair, A. (2024). Protecting dignity in the digital age: Deepfakes and Indian criminal law reform. *National Law School of India Review, 36*(1), 45–76.
- Green, M., & Narayanan, A. (2020). How to recognize a deepfake. *Scientific American, 323*(6), 26–29.
- Jain, S. (2024). Privacy and deepfakes: The evolving Indian jurisprudence. *Indian Law Review, 8*(2), 112–145.
- Kapoor, R. (2025). Regulating synthetic media: Lessons from comparative jurisdictions. *Journal of International Media & Policy, 12*(1), 89–118.
- McGlynn, C., Rackley, E., & Houghton, R. (2021). Beyond revenge porn: The continuum of image-based sexual abuse. *Feminist Legal Studies, 29*(1), 25–46.
- Narain, A. (2025). India's data protection landscape post-Puttaswamy. *Indian Journal of Constitutional Law, 19*(1), 33–61.
- Ohm, P. (2010). Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA Law Review, 57*(6), 1701–1777.
- Rosen, J. (2012). The right to be forgotten. *Stanford Law Review Online, 64*(88), 88–92.
- Scherer, M. (2016). Regulating artificial intelligence systems: Risks, challenges, and opportunities. *Harvard Journal of Law & Technology, 29*(2), 353–400.
- Schulhofer, S. J. (2018). The dignity of privacy in an era of deep surveillance. *University of Chicago Law Review, 85*(3), 1–44.
- Wagner, B. (2021). Fundamental rights and the governance of AI. *European Law Journal, 27*(3), 356–375.
- Zuboff, S. (2019). *The age of surveillance capitalism.* New York: Public Affairs.

News and Practitioner Sources

- Christopher, N. (2020, February 18). We've just seen the first use of deepfakes in an Indian election campaign. *VICE News.*
- NDTV. (2020, February 19). BJP shared deepfake video during Delhi election campaign. *NDTV News.*
- Reporters Without Borders. (2023). Rana Ayyub, the face of India's women journalists plagued by cyber harassment. *RSF Report.*
- The Hindu. (2025, March 12). Parliamentary panel calls for stringent laws on deepfakes. *The Hindu.*
- The Verge. (2020, February 18). An Indian politician used AI to translate his speech. *The Verge.*
- Times of India. (2025, August 10). Odisha Police to establish dedicated cybercrime unit. *Times of India.*
- Wired. (2024, May 20). Indian voters bombarded with millions of deepfakes. *Wired Magazine.*
- World Economic Forum. (2022). *Global risks report: Misinformation and deepfakes.* Geneva: WEF.

EDITORIAL TEAM

INTERNATIONAL EDITORIAL TEAM

ABOUT LEX SCRIPTA JOURNAL

Lex Scripta Magazine is a premier peer-reviewed online and print journal dedicated to advancing scholarly research in law, policy, and social sciences. With the vision of promoting academic excellence and fostering a culture of intellectual exchange, the magazine provides a distinguished platform for academicians, researchers, legal professionals, and students to publish their original work and contribute to contemporary legal discourse.

Each submission undergoes a rigorous double-blind review process conducted by a panel of eminent national and international professors, ensuring the highest standards of quality and academic integrity. Lex Scripta not only encourages original and innovative research but also strives to bridge the gap between theoretical insights and real-world applications in the legal domain.

Contributors and editorial members receive global recognition through certificates and publication opportunities, while readers gain access to insightful, authoritative, and thought-provoking content across diverse areas of law and policy.

Now managed by Integrity Education India, Lex Scripta Magazine is committed to expanding its academic footprint through enhanced digital presence, global collaborations, and university partnerships. Upholding its ISSN identity, Lex Scripta continues to evolve as one of India's most trusted and respected journals in the field of legal research and education.

KEY FEATURES

- **Scholarly Insights** – Access in-depth, peer-reviewed research articles written by distinguished academicians and legal experts.
- **Global Perspectives** – Explore diverse viewpoints on law, policy, and governance from national and international scholars.
- **Authentic Content** – Read verified and academically sound articles that uphold the highest standards of research quality.
- **Knowledge Enhancement** – Stay updated with emerging trends, case studies, and policy developments across multiple legal domains.
- **Easy Accessibility** – Enjoy seamless access to online editions and exclusive hardcover issues for academic and professional use.

LEX SCRIPTA JOURNAL
JOURNAL MAGAZINE BY INTEGRITY EDUCATION INDIA

CONNECT WITH US 9811 666 216
7011 605 618