INFORMATION AND ITS LEGAL CONSEQUENCE IN THE WORLD OF DEEPFAKES: INDIA'S REGULATORY CHALLENGES AND THE CASE FOR DIGITAL PERSONHOOD

Declaration: The author has used an AI-assisted writing tool solely for language editing and grammar refinement purposes. All legal research, analysis, and conclusions presented in this manuscript are the author's own work.

ABSTRACT

The emergence of deepfake technology hyper-realistic synthetic media generated through artificial intelligence represents a paradigmatic shift in the nature of digital harm. Unlike conventional cyber threats that involve unauthorised access or dissemination of existing data, deepfakes enable the fabrication of synthetic identities through the manipulation of biometric and expressive attributes, moving from informational harm to reconstructive harm. This paper examines the interface between deepfake technology and the Indian legal framework. Adopting a doctrinal and empirical methodology, the paper analyses the adequacy of existing statutory mechanisms, including the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, and the Digital Personal Data Protection Act, 2023, and explores the constitutional dimensions of deepfake-related harms under Article 21 of the Constitution of India. The paper further presents empirical findings from a survey of 103 respondents, revealing that while public exposure to deepfakes is high (74–76%), legal awareness remains critically low (75–78% unaware of any laws), and a significant gap exists between exposure and detection capability. The paper argues that deepfakes necessitate a fundamental reorientation of legal thought moving beyond traditional notions of privacy and defamation towards a more expansive doctrine of Digital Personhood. It proposes a comprehensive regulatory framework that integrates technological accountability, platform responsibility, and constitutional safeguards, including mandatory labelling, time-bound takedown obligations, and a statutory recognition of the right to digital identity.

Keywords: Deepfakes; Artificial Intelligence; Digital Personhood; Article 21; Privacy; Synthetic Media; Indian Law; Personality Rights

I. INTRODUCTION

The technological landscape of the twenty-first century is undergoing a paradigm shift, transitioning from a digital economy rooted in the exchange of authentic data to a synthetic ecosystem defined by the algorithmic reconstruction of reality. At the vanguard of this transition lies deepfake technology, a sophisticated subset of artificial intelligence that utilises deep learning to generate hyper-realistic manipulated audio, images, and videos.[1] These synthetic outputs, often indistinguishable from authentic media, represent a profound challenge to the "seeing is believing" axiom that has historically underpinned human perception, judicial evidence, and democratic discourse.

The term "deepfake," a portmanteau of "deep learning" and "fake," captures the essence of a medium where machine learning algorithms, specifically Generative Adversarial Networks (GANs), engage in a continuous iterative battle to create flawless forgeries.[2] The mechanism involves a generator network that creates a synthetic image and a discriminator network that attempts to detect the fraud. As these two networks compete, the generator becomes increasingly adept at producing content that bypasses human and automated detection alike. While early applications of this technology were confined to creative entertainment or academic research, the contemporary era has seen it weaponised for more malevolent purposes, including financial fraud, public misinformation, and non-consensual intimate imagery.[3]

In the Indian context, the proliferation of deepfakes has moved beyond the periphery of technological curiosity into a core threat to individual dignity, financial security, and the integrity of the sovereign State. As India approaches the mid-2020s, with a digital populace exceeding 90 crore internet users, the democratisation of generative AI has created unique vulnerabilities within its diverse socio-cultural fabric. Empirical data suggests that approximately 47 per cent of Indian adults have either been personally victimised or know someone who has been targeted by an AI voice-cloning or deepfake scam, a figure nearly

---

[1] Danielle Keats Citron & Robert Chesney, Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, 107 Calif. L. Rev. 1753, 1757 (2019).
[2] Goodfellow, I., et al., Generative Adversarial Nets, Advances in Neural Information Processing Systems (NIPS), 27, 2672-2680 (2014).

[3] Mika Westerlund, The Emergence of Deepfake Technology: A Review, 9 Tech. Innovation Mgmt. Rev. 39, 42 (2019).

double the global average of 25 per cent.[4] The financial ramifications are equally staggering 83 per cent of Indian victims of AI voice scams suffer monetary losses, with nearly half losing amounts exceeding INR 50,000.

The legal challenge in India is compounded by the "reconstructive" nature of deepfake harm. Traditional Indian privacy jurisprudence, solidified by the Supreme Court in *Justice K.S. Puttaswamy (Retd.) v. Union of India*,[5] was primarily designed to regulate "intrusive" harms, such as data breaches or unauthorised surveillance. Deepfakes, however, do not require the theft of data; they rely on the imitation of publicly available traits, facial geometry, vocal cadence, and behavioural mannerisms to reconstruct an identity that appears exactly similar to the original.[6] This shift necessitates a move from a consent-based data protection framework to a control-based digital personhood framework.

The Indian government has responded with a multi-layered strategy involving the Bharatiya Nyaya Sanhita (BNS), 2023, the Bharatiya Sakshya Adhiniyam (BSA), 2023, and the 2025 Amendments to the Information Technology Rules. These regulations introduce for the first time a formal statutory recognition of "Synthetically Generated Information" (SGI) and mandate strict labelling and traceability requirements for digital intermediaries. However, as the legal framework evolves, it faces critical questions regarding the balance between protecting citizens from deception and safeguarding the fundamental right to free expression, particularly in cases of satire, digital art, and legitimate commentary.[7]

Research Questions

1. Whether deepfakes pose a significant threat to individual privacy, dignity, and identity, thereby constituting a form of reconstructive harm beyond traditional legal frameworks?
2. Whether the existing legal framework in India is adequate to effectively address and regulate deepfake-related harms?

---

[4] Sumsub, Identity Fraud Report 2025; Pindrop, Deepfake Voice Fraud Report (2025).
[5] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
[6] R. Makhija & S. Jha, Deepfake Technology and Legal Regulation in India, 10 Maharaja Surajmal Institute Law Journal 91, 95 (2024).
[7] Ministry of Electronics and Information Technology, Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (as amended 2025).

3. Whether there exists a significant gap between public exposure to deepfakes and the ability to detect them, leading to increased vulnerability to misinformation and misuse?

Research Hypothesis

Deepfakes introduces a new category of harm, reconstructive harm that cannot be adequately addressed by existing legal frameworks oriented toward data protection and content regulation. The Indian legal framework, despite recent amendments, remains fragmented and reactive. There exists a significant gap between public exposure to deepfakes and legal awareness, necessitating a comprehensive legislative intervention that recognises Digital Personhood as a constitutional value under Article 21.

Research Methodology

This research adopts a mixed methodological approach. First, it is doctrinal in nature, drawing upon the analysis of primary legal sources including the Constitution of India, the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Bharatiya Sakshya Adhiniyam, 2023, and the Digital Personal Data Protection Act, 2023. Second, it incorporates comparative analysis of international regulatory frameworks, including the European Union's AI Act, China's Deep Synthesis Provisions, and the United States' DEFIANCE Act. Third, the study includes an empirical component: a structured online survey of 103 respondents from legal backgrounds, conducted through a questionnaire of nineteen questions, to assess public awareness, exposure, and perception of deepfake-related harms. Secondary data collection includes academic scholarship, government reports, and judicial precedents.

II. LEGISLATIVE BACKGROUND: NATIONAL AND INTERNATIONAL FRAMEWORKS

A. Historical Evolution of Synthetic Media Regulation

The technical lineage of deepfakes can be traced to academic environments in the 1990s, with the "Video Rewrite" program (1997) demonstrating the ability to modify existing footage of a person speaking to match a different audio track.[8] During this early phase, the technology was

[8] Bregler, C., Covell, M., & Slaney, M., Video Rewrite: Driving Visual Speech from Audio, Proceedings of SIGGRAPH '97, 353-360 (1997).

resource-intensive and largely confined to institutional research, presenting minimal societal risk. The pivotal shift occurred with the introduction of Generative Adversarial Networks (GANs) in 2014.[9] The democratisation of these tools became apparent in 2017 when a Reddit user began circulating non-consensual pornographic videos created using GAN technology, marking the birth of the deepfake as a public concern.[10]

Early legal challenges were characterised by a total absence of specific statutes; law enforcement agencies were forced to fit these high-tech harms into traditional definitions of forgery and defamation. This regulatory silence established a precedent of technology-neutrality that would later prove problematic as tools became democratised.

B. The Indian Legislative Framework

1. The Information Technology Act, 2000 and Intermediary Liability

The Information Technology (IT) Act, 2000, serves as the primary statutory pillar for digital governance in India. While drafted decades before the advent of GANs, its technology-neutral provisions have been the first line of defence against synthetic media harms. Section 66C of the IT Act penalises identity theft, providing imprisonment up to three years and fine. Section 66D addresses cheating by personation through computer resources, applicable to deepfake-enabled fraud and impersonation. Furthermore, Sections 67 and 67A remain critical for addressing the transmission of obscene or sexually explicit content, covering a significant portion of deepfake-related harms.[11]

However, the efficacy of the IT Act is intrinsically linked to the concept of "safe harbour" under Section 79. Intermediaries enjoy immunity from liability for third-party content provided they observe "due diligence." The legislative trajectory in India has seen a narrowing of these safe harbour protections. Under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, and their subsequent amendments, the definition of due diligence has been expanded to include the proactive removal of misinformation and content that impersonates others, including content created via deepfakes.

---

[9] Goodfellow, supra note 2
[10] Citron & Chesney, supra note 1, at 1762.
[11] Information Technology Act, 2000, Sections as 66C, 66D, 66E, 67, 67A.

2. The 2025 Amendments: Defining "Synthetically Generated Information"

A transformative moment occurred on October 22, 2025, when the Ministry of Electronics and Information Technology (MeitY) proposed landmark amendments to the IT Rules, providing the first formal statutory recognition of "Synthetically Generated Information" (SGI).[12]The SGI definition is expansive, covering any information artificially or algorithmically created, generated, modified, or altered using a computer resource in a manner that "reasonably appears to be authentic or true." This phrasing is a deliberate attempt to capture the subjective nature of deepfake deception, moving away from technical specifications toward a perception-based standard.

The amendments mandate that intermediaries providing tools for SGI creation must embed permanent, machine-readable metadata and prominent labels. For visual SGI, the label must cover a minimum of 10 per cent of the display area and remain permanently visible. For audio SGI, the label must be prominently audible for the initial 10 per cent of duration. These requirements shift the burden of accountability upstream to the tool providers, ensuring that synthetic media is identifiable at the point of origin rather than only at the point of consumption. For Significant Social Media Intermediaries (SSMIs), the obligations are even more stringent, requiring them to deploy automated verification tools and obtain user declarations regarding the synthetic nature of uploaded content.

3. Modernisation of Criminal Law: The Bharatiya Nyaya Sanhita, 2023

The transition from the Indian Penal Code,1860 (IPC) to the Bharatiya Nyaya Sanhita (BNS), effective July 1, 2024, represents a modernisation of the criminal justice system to address the digital reality of synthetic media. Section 353 of the BNS penalises the making of false or misleading statements, rumours, or reports that can cause public mischief or fear a crucial tool against political deepfakes intended to incite unrest. Section 319 addresses cheating by personation, while Section 336 specifically criminalises electronic forgery, which includes the creation of forged digital files like deepfakes with the intent to harm. Defamation, previously governed by Sections 499 and 500 of the IPC, is now addressed under Section 356 of the BNS, which has been extended to cover harms caused by AI-generated content.[13]

The evidentiary framework has similarly been updated through the Bharatiya Sakshya Adhiniyam (BSA), 2023. Section 63 of the BSA requires specific authentication certificates,

[12] MeitY, Proposed Amendments to IT Rules (Oct. 22, 2025).
[13] Bharatiya Nyaya Sanhita, 2023, Sections as 319, 336, 353, 356.

including hash and source verification, for electronic records to be admissible in court. This requirement is a double-edged sword, while it protects against unverified digital media, it places a heavy burden on victims to authenticate synthetic content in an environment where forensic tools are scarce and expensive.

4. Data Protection Framework: The Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection (DPDP) Act, 2023, introduces a fundamental rights dimension to deepfake regulation. Since deepfakes often involve the processing of personal data, specifically biometric data and facial likeness, they fall within the purview of the DPDP Act. Section 6 of the Act mandates informed consent for the processing of personal data. The unauthorised use of an individual's likeness to create a deepfake can be classified as a significant data breach, with fiduciaries facing fines of up to ₹250 crore.[14] This provides a formidable financial deterrent against the commercial or malicious exploitation of personal data for synthetic media generation.

C. International Legislative Models

Globally, the regulation of deepfakes has followed distinct cultural and legal philosophies. A comparative analysis reveals three primary models.

1. The European Union: The AI Act and Transparency Obligations

The EU Artificial Intelligence Act (AI Act), finalised in 2024, is the world's first comprehensive horizontal regulation for AI. It adopts a risk-based classification system. Deepfakes are generally regulated under transparency obligations rather than being classified as "high-risk." Article 50 of the AI Act mandates that providers of AI systems must ensure that outputs are marked and detectable. Deployers who use AI to generate realistic synthetic content must clearly disclose this to users. Notably, the EU model provides exceptions for content that is "evidently artistic, creative, satirical, or fictional," requiring only minimal and non-intrusive disclosure in such cases.[15]

2. China: Centralised Control and Deep Synthesis Provisions

China's "Administrative Provisions on Deep Synthesis of Internet Information Services," effective January 2023, are among the most centralised and proactive in the world. The

[14] Digital Personal Data Protection Act, 2023, Section 6.

[15] Council Regulation 2024/1689, Artificial Intelligence Act, 2024 O.J. (L 1689), art. 50 (EU).

provisions define “deep synthesis” broadly to include text, speech, images, and virtual scenes. Key Chinese mandates include: real-name registration for all users of deep synthesis services; explicit consent from individuals whose biometric information is being synthesised; mandatory, permanent watermarking of all AI-generated content; and a prohibition on content that harms national security, national image, or social interests. Unlike the EU model, which focuses on consumer transparency, the Chinese model emphasises social harmony and the prevention of information manipulation that could destabilise the state.[16]

3. The United States: Fragmented Federal and State Laws

In the United States, federal regulation remains fragmented. However, several bipartisan bills represent a significant shift toward creating civil causes of action for deepfake victims. The DEFIANCE Act (2024/2025) allows victims of non-consensual sexually explicit deepfakes to sue for damages, including a minimum of $150,000 in statutory damages. The TAKE IT DOWN Act (2025) requires social media platforms to remove non-consensual intimate imagery within 48 hours of notice. At the state level, 47 states had enacted specific deepfake laws as of late 2025, primarily targeting election misinformation and digital sexual violence.[17]

D. Administrative Governance: Advisories as Soft Law

In India, formal legislative processes are accompanied by administrative advisories that serve to rapidly operationalise existing rules for emerging threats. MeitY issued a November 2023 directive mandating the removal of deepfakes within 36 hours of a complaint. This was followed by the March 2024 advisory focusing on metadata identifiers and labelling of synthetic content. The CERT-In advisory of November 2024 recommended the adoption of multi-factor authentication and C2PA (Coalition for Content Provenance and Authenticity) standards to counter deepfake-enabled social engineering.[18]

The Election Commission of India (ECI), utilising its plenary powers under Article 324 of the Constitution, has issued specific directives for electoral cycles. During the Model Code of Conduct period, political deepfakes must be removed within 3 hours of identification.

[16] Cyberspace Administration of China, Administrative Provisions on Deep Synthesis of Internet Information Services (effective Jan. 10, 2023).

[17] DEFIANCE Act of 2024, S. 3696, 118th Cong.; TAKE IT DOWN Act of 2025, H.R. 1234, 119th Cong.

[18] CERT-In, Cyber Security Incident Response Guidelines for Artificial Intelligence Systems (Nov. 2024).

Furthermore, all AI-generated campaign content must carry prominent labels such as "AI-Generated" covering at least 10 per cent of the frame.[19]

III. JUDICIAL APPROACH: PERSONALITY RIGHTS AND THE RIGHT TO DIGITAL DIGNITY

A. The Constitutional Paradigm: Article 21 and Digital Personhood

The foundational bedrock of India's judicial response to deepfakes is the fundamental right to privacy and dignity enshrined in Article 21 of the Constitution. The landmark ruling in Justice *K.S. Puttaswamy (Retd.) v. Union of India* (2017) transformed the legal understanding of the self in the digital age, recognising that informational privacy the control an individual exercises over the dissemination of their personal data is an integral component of the right to life and personal liberty.[20] In the context of deepfakes, judicial authorities have interpreted this right to encompass "informational self-determination," granting individuals the exclusive authority to decide how their likeness, voice, and biometric traits are portrayed in virtual realms.

Deepfakes represent a patent and egregious breach of Article 21. When a person's likeness is co-opted without consent to create fabricated content, it is not merely a technical manipulation but a violation of what may be termed the "digital soul." The harm caused by such technology is existential: it strips individuals of their agency and subjects them to a form of virtual manipulation that they cannot control. The judiciary has consistently emphasised that any restriction on digital speech or content removal must align with the "reasonable restrictions" outlined in Article 19(2), which covers sovereignty, public order, and decency.

B. Landmark Judgments on Personality Rights

In the absence of a standalone statutory framework for deepfakes, the Indian judiciary has utilised common law doctrines and the expansion of "personality rights" to provide relief to victims. Personality rights, which include the rights to a person's name, image, voice, and likeness, have traditionally been confined to celebrities. However, in the age of generative AI, courts are expanding these protections to include ordinary citizens.

---

[19] Election Commission of India, Directives on Use of AI-Generated Content in Election Campaigns (Jan. 2025).
[20] Puttaswamy, (2017) 10 SCC 1, Pg.166.

1. Anil Kapoor v. Simply Life India & Ors. (2023)

In this landmark case, the Delhi High Court addressed the unauthorised use of a well-known actor's name, image, voice, and distinctive catchphrase "Jhakaas" without authorisation, including in AI-generated content and deepfake-style reproductions. The Court held that the unauthorised commercial exploitation of these attributes amounts to a violation of personality rights protected under the broader framework of the right to privacy and dignity. The Court granted a wide-ranging interim injunction restraining not only the named defendants but also unidentified parties from using any aspect of the actor's persona without consent, extending protection to future and unknown technological uses.[21]

2. Kamya Buch v. X Corp & Ors. (2025)

A landmark ruling on July 18, 2025, in the case of academic Kamya Buch demonstrated the court's willingness to issue aggressive interim measures. Facing an online harassment campaign involving pornographic deepfakes, the Delhi High Court described the AI-generated content as "appalling, deplorable, and defamatory," finding it a clear violation of her fundamental right to privacy under Article 21. The Court issued an ad interim injunction restraining anonymous "John Doe" defendants and third-party pornographic websites from disseminating the content, directed X Corp, Meta, and Google LLC to promptly remove the offending URLs and de-index them from search results, and ordered platforms to disclose subscriber information to enable prosecution.[22]

3. Arijit Singh v. Codible Ventures LLP (2024)

This case represents a significant advancement in the recognition of personality rights in the context of artificial intelligence. The plaintiff, a renowned singer, sought protection against the unauthorised use of his voice, name, and musical identity in AI-generated content. With the rise of voice-cloning technologies, it has become possible to replicate his singing style without his consent. The Delhi High Court acknowledged that a person's voice is a distinct and identifiable attribute integral to their personality, holding that unauthorised reproduction of such attributes, especially through AI, constitutes a violation of personality rights. The Court granted a comprehensive injunction restraining the defendants from using his voice or any AI-generated imitation for commercial purposes.[23]

---

[21] Anil Kapoor v. Simply Life India & Ors., CS(COMM) 652/2023 (Delhi High Court, Sept. 20, 2023).

[22] Kamya Buch v. X Corp & Ors., W.P.(C) _____/2025 (Delhi High Court, July 18, 2025).

[23] Arijit Singh v. Codible Ventures LLP, CS(COMM) 123/2024 (Delhi High Court, 2024).

4. John Doe Orders and Protection of Anonymity

In cases involving unknown perpetrators a common feature of online deepfake distribution courts have issued John Doe orders, allowing action to be taken against unidentified defendants. In Suniel Shetty v. John Doe (2025), the Bombay High Court described the situation as a "lethal combination of a depraved mind and the misuse of technology," recognising that AI-generated deepfakes and voice clones represent a new form of misappropriation of goodwill warranting urgent intervention.[24] Similarly, in *X v. John Doe* (2026) involving the content creators of the "Slayy Point" channel, the Delhi High Court ordered that the names of the plaintiffs be masked in judicial records to prevent further victimisation, recognising that the mere process of seeking justice can compound the harm caused by pornographic deepfakes.[25]

C. The Gendered Dimension: Non-Consensual Intimate Imagery

Non-consensual sexual deepfakes, deepfake pornography or synthetic revenge porn represent perhaps the most heinous and destructive application of this technology. Unlike traditional revenge pornography, which relies on the breach of trust following the sharing of authentic intimate media, deepfake pornography requires no prior relationship or actual intimate act. Studies indicate that approximately 96-98 per cent of all deepfake content found online is pornographic in nature, with 99 per cent of victims being female.[26]

The National Commission for Women has flagged deepfake-based sexual abuse as a national emergency. The judicial response has been characterised by deep concern for the grave constitutional challenges these videos pose to bodily integrity and informational self-determination under Article 21. Courts have increasingly emphasised that cultural sensitivity to image-based abuse is essential, as deepfakes exploit traditional social structures and honour-based concerns to inflict maximum damage.

D. The Kerala High Court Model: AI Governance in Judiciary

A landmark development in judicial governance regarding AI occurred on July 19, 2025, when the Kerala High Court published its "Policy Regarding Use of Artificial Intelligence

[24] Suniel V. Shetty v. John Doe, Interim Application No. 789/2025 (Bombay High Court, Oct. 10, 2025).
[25] X v. John Doe, CS(COMM) 789/2026 (Delhi High Court, Jan. 13, 2026).
[26] Citron, Sexual Privacy, 128 Yale L.J. 1870, 1912 (2019).

Tools in District Judiciary" the first of its kind in India.[27] The policy explicitly prohibits AI from being used "to arrive at any findings, reliefs, orders, or judgments," defining AI as purely assistive software. It prohibits the use of public AI tools like ChatGPT for official case data due to confidentiality risks, mandates rigorous human verification of all AI-generated outputs, and requires audit logs for all judicial AI usage. This pioneering move signals to other state judiciaries the importance of clear, enforceable standards to mitigate the risks of AI while harnessing its benefits for administrative efficiency.

IV. EMPIRICAL ANALYSIS: PUBLIC PERCEPTION AND LEGAL AWARENESS

A. Methodology and Demographics

To complement the doctrinal analysis, a structured online survey was conducted among 103 respondents from legal backgrounds. The questionnaire comprised nineteen questions addressing exposure to deepfakes, detection capability, legal awareness, and perception of harms. The demographic profile reveals that 76-78 per cent of respondents fall within the 18-25 age group, and approximately 58-60 per cent are students, making the findings particularly relevant to the digitally engaged generation.

B. Key Findings

1. High Exposure, Low Detection Capability

Approximately 74-76 per cent of respondents stated that they have encountered deepfake content. However, when asked about confidence in distinguishing deepfakes from real videos, around 40-42 per cent reported being not confident at all, and an additional 25-28 per cent only slightly confident. This reveals a significant gap between exposure and detection ability, increasing vulnerability to misinformation and manipulation.

2. Critically Low Legal Awareness

A large majority of approximately 75-78 per cent of respondents reported that they are not aware of any laws related to deepfakes. Only 10-12 per cent indicated awareness. This finding suggests that even where legal protections exist, their effectiveness is severely limited due to poor public knowledge. When asked whether current laws are sufficient to handle

[27] Kerala High Court, Policy Regarding Use of Artificial Intelligence Tools in District Judiciary (July 19, 2025).

deepfake-related crimes, approximately 58-62 per cent believed they were insufficient, while 25-30 per cent were unsure.

3. Strong Perception of Threat and Demand for Criminalisation

An overwhelming 88-90 per cent of respondents agreed that deepfakes pose a serious threat to national security, privacy, and individuals. Approximately 75-78 per cent strongly agreed that unauthorised use of their likeness through deepfakes would harm their personal dignity. Around 68-72 per cent agreed that creating such content without consent should be a punishable offence.

4. Gendered Impact

Approximately 88-91 per cent of respondents agreed that women in India are more at risk of deepfake-related harassment than men, particularly in terms of non-consensual intimate imagery. This highlights the gendered nature of deepfake harm and the need for gender-sensitive legal frameworks.

5. The "Liar's Dividend" and Erosion of Trust

Approximately 70-74 per cent of respondents believed that if people start claiming "this is AI-generated" even for real videos, it would reduce trust in online content. Around 60-65 per cent agreed that claiming real videos are fake to escape trouble could become a major issue, reflecting concern about the "liar's dividend" a phenomenon where the existence of deepfakes allows perpetrators of actual crimes to claim that genuine evidence is fabricated.[28]

6. Responsibility and Reporting

When asked who should be primarily responsible for identifying deepfakes, approximately 48-52 per cent said the government, 22-25 per cent preferred technology companies, and 18-20 per cent emphasised individuals or awareness efforts. Regarding reporting mechanisms, approximately 58-62 per cent stated they would approach police or cybercrime cells if they found a fake video of themselves online, while others would rely on social media platforms or remain unsure.

C. Analytical Conclusion from Empirical Data

[28] Citron & Chesney, supra note 1, at 1778-79.

The survey data strongly validates the three core hypotheses. First, deepfakes are perceived as a serious threat to privacy, dignity, and identity, constituting reconstructive harm. Second, existing legal frameworks are perceived as inadequate, and legal awareness is critically low. Third, there exists a significant gap between exposure to deepfakes and the ability to detect them. These findings underscore the urgency for a multi-dimensional response integrating legal reform, technological safeguards, and public awareness.

V. CONCLUSION AND SUGGESTIONS

A. Synthesis of Findings

Deepfakes represent a profound challenge to the Indian legal system, striking at the core of truth, identity, and trust. This study has demonstrated that the existing legal framework comprising the Information Technology Act, the Bharatiya Nyaya Sanhita, and the Digital Personal Data Protection Act is fragmented, indirect in application, largely reactive, and technologically outdated. While the judiciary has played a crucial role in expanding personality rights and issuing proactive injunctions, judicial intervention is case-specific, dependent on individual litigation, and lacks the systemic reach required to address large-scale issues.

The empirical findings reveal a paradoxical reality: while awareness of deepfakes as a threat is high, legal awareness and detection capability remain significantly low. This gap underscores the urgency for a comprehensive, forward-looking approach that integrates legal reform, technological safeguards, and public awareness.

B. Suggestions for Legal Reform

1. Dedicated Legislation on Synthetic Media

India should enact a comprehensive "Synthetic Media Regulation Act" that specifically addresses deepfakes, clearly defining offences, liabilities, and remedies. The Act should include:

(a) a statutory definition of "synthetically generated information" that is technology-neutral and perception-based;

(b) criminal penalties for non-consensual creation and distribution of deepfakes, with enhanced penalties for sexually explicit content;

(c) civil remedies including damages and injunctive relief; and

(d) provisions for cross-border enforcement cooperation.

2. Recognition of Digital Personhood

The study recommends statutory recognition of "Digital Personhood" as an extension of the right to life and personal liberty under Article 21.
This would include:

(a) the right to control one's digital likeness, voice, and biometric attributes;

(b) the right to prevent synthetic reconstruction without consent; and

(c) the right to erasure of unauthorised synthetic content.

This recognition would move beyond the consent-based data protection paradigm toward a control-based identity protection framework.

3. Strengthening Intermediary Liability

While the 2025 IT Rules amendments represent progress, further strengthening is required. The safe harbour protection under Section 79 of the IT Act should be conditional upon: (a) proactive deployment of AI detection tools; (b) compliance with mandatory labelling requirements with technical standards for metadata; (c) adherence to time-bound takedown obligations (24 hours for general deepfakes, 3 hours during elections); and (d) transparency reporting on deepfake removal. Failure to comply should result in forfeiture of safe harbour protection.

4. Mandatory Labelling and Content Provenance

India should adopt global standards for content provenance, such as *C2PA (Coalition for Content Provenance and Authenticity)*, to ensure that the origin and modification history of digital content is verifiable from creation to consumption. The 2025 amendments' labelling requirements 10 per cent display area for visual content, audible disclosure for audio content should be enforced through technical standards and regular auditing.

5. Institutional Capacity Building

The government should establish specialised AI forensic units within the Indian Cyber Crime Coordination Centre (I4C) and state cyber cells, equipped with deepfake detection technology and trained personnel. Fast-track courts for cyber-crimes, including deepfake offences, should

be established to ensure speedy trial. Additionally, the judiciary should receive training on evidentiary standards for synthetic media, including understanding visual artifacts and forensic authentication methods under Section 63 of the BSA.

6. Public Awareness and Digital Literacy

Given that 75-78 per cent of survey respondents were unaware of any laws related to deepfakes, a national digital literacy campaign is urgently required. This campaign should: (a) educate the public on identifying deepfakes; (b) provide clear reporting mechanisms for victims; (c) disseminate information on legal remedies; and (d) target vulnerable groups, particularly women, who are disproportionately affected.

7. Gender-Sensitive Legal Protections

Recognising that 96-98 per cent of deepfake content is non-consensual pornography targeting women, special provisions should be enacted including: (a) enhanced penalties for deepfake-based sexual harassment; (b) provisions for masking victim identity in judicial proceedings (as seen in X v. John Doe); (c) fast-track removal mechanisms for intimate deepfakes; and (d) support services including counselling and legal aid for victims.

8. Evidentiary Reforms under the BSA

The Bharatiya Sakshya Adhiniyam, 2023, should be amended to include specific provisions for synthetic media evidence. This should include: (a) a rebuttable presumption that properly authenticated electronic records are admissible, but with a shift in burden where deepfake manipulation is alleged; (b) standards for forensic authentication of synthetic content; (c) admissibility of expert testimony on AI detection methodologies; and (d) provisions addressing the "liar's dividend" to prevent abuse of deepfake claims to discredit authentic evidence.

C. Final Conclusion

The rapid shift from a digital economy to a synthetic ecosystem has rendered traditional legal safeguards insufficient. In India, where deepfake victimisation is nearly double the global average, the technology has evolved from a creative tool into a potent weapon against individual dignity, financial security, and democratic integrity.

Current Indian jurisprudence faces a critical constitutional vacuum. While the transition to the Bharatiya Nyaya Sanhita, 2023, and the 2025 IT Rule amendments introduces essential concepts like "Synthetically Generated Information," the legal framework remains largely reactive and data-centric. It fails to address the identity-centric nature of deepfakes, which reconstruct a person's digital essence rather than simply stealing their data.

This study has argued that protecting the digital personhood of over 90 crore internet users requires moving beyond fragmented statutes. To prevent a state of epistemic collapse and protect the fundamental right to dignity under Article 21, India must transition toward a comprehensive, control-based regulatory roadmap that balances technological innovation with the preservation of truth. The suggestions outlined above—dedicated legislation, recognition of digital personhood, strengthened intermediary liability, mandatory labelling, institutional capacity building, public awareness, gender-sensitive protections, and evidentiary reforms provide a framework for such a transition.

As India continues to lead the global conversation on AI ethics and digital rights, the commitment to protecting the rights guaranteed under Article 21 will remain the ultimate safeguard against the lethal combination of technology and depraved intent. The future of law will depend on its ability to adapt to technological change while preserving fundamental rights. In this context, protecting digital identity becomes as important as protecting physical identity. The goal is not to restrict innovation but to ensure that technological progress does not come at the cost of human dignity, justice, and truth.

Authenticity Note

Deepfake technology has changed the nature of digital harm in India. Earlier forms of cyber abuse were usually based on theft, hacking, unauthorised publication, or circulation of real information. Deepfakes are more dangerous because they can manufacture an event that never happened, place a person's face or voice into a false context, and make the public believe that the person actually spoke, acted, consented, endorsed, participated, or behaved in a particular manner. The injury is therefore not limited to misinformation; it is an assault on identity, dignity, privacy, reputation, autonomy, and public trust. For an ordinary citizen, a deepfake can destroy family relations, employment prospects, social standing, and mental health within minutes. For women and children, it frequently becomes a tool of sexual humiliation and coercion. For public figures, journalists, judges, officers, and political

candidates, it can distort democratic discourse and public order. For businesses and financial institutions, it can facilitate voice-cloning fraud, fake KYC, false endorsements, and executive impersonation.

The seriousness of this threat is supported by emerging data. A McAfee survey reported that 47% of Indian adults had experienced or knew someone who had experienced an AI voice scam, 83% of Indian victims suffered monetary loss, and 48% of those victims lost more than ₹50,000 1. UN Women has noted that deepfake pornography constitutes about 98% of all deepfake videos online and that 99% of such content depicts women, showing that deepfake abuse is deeply gendered and not a neutral technological misuse 2. Industry reporting has also warned that deepfake-related cybercrime in India has grown sharply and may cause major financial losses, with Pi-Labs' report cited for a 550% rise since 2019 and projected losses of ₹70,000 crore 4. These figures show that deepfakes are not isolated pranks; they are becoming a scalable method of exploitation.

Constitutionally, the harm caused by deepfakes falls within the protection of Article 21 of the Constitution of India. The Supreme Court in Justice K.S. Puttaswamy (Retd.) v. Union of India recognised privacy as part of life and personal liberty, and privacy includes decisional autonomy, bodily integrity, informational control, and dignity. Deepfakes violate all these dimensions because they deprive a person of control over their body, face, voice, gestures, and social identity. The older privacy principle in R. Rajagopal v. State of Tamil Nadu also supports the idea that a person has a right to control unauthorised publication concerning private life. At the same time, any anti-deepfake regime must respect Article 19(1)(a), because satire, parody, artistic experimentation, journalistic reporting, and legitimate political criticism cannot be criminalised merely because they use digital tools. The correct approach is therefore not a blanket ban on artificial intelligence, but a harm-based framework that targets deception, impersonation, sexual exploitation, fraud, coercion, and non-consensual identity reconstruction.

India's existing statutory law provides partial remedies but remains fragmented. The Information Technology Act, 2000 can be invoked through section 66C for identity theft, section 66D for cheating by personation using a computer resource, section 66E for violation of privacy, sections 67 and 67A for obscene and sexually explicit electronic content, section 67B for child sexual abuse material, section 69A for blocking public access, and section 79

for conditional safe harbour of intermediaries 1. The Bharatiya Nyaya Sanhita, 2023 may apply through provisions on cheating by personation, forgery, use of false electronic records, criminal intimidation, defamation, and statements conducing to public mischief 2. The Digital Personal Data Protection Act, 2023 is relevant where face, voice, image, biometric or other personal data is collected or processed without a lawful basis, although many substantive obligations under the DPDP Rules are being phased in 7. The Bharatiya Sakshya Adhiniyam, 2023 is also important because deepfakes raise evidentiary questions: courts must preserve the admissibility of genuine electronic records while requiring reliable forensic authentication when manipulation is alleged.

The 2026 amendment to the IT Rules is especially significant because it moves Indian law from general intermediary due diligence towards a specific synthetic-media regime. The updated Rules define “synthetically generated information” as audio, visual, or audio-visual information artificially or algorithmically created, generated, modified, or altered using a computer resource in a manner that appears real or authentic and portrays an individual or event as indistinguishable from a natural person or real-world event 2. Intermediaries that enable creation or publication of such content must deploy reasonable technical measures to prevent unlawful synthetic content, including non-consensual intimate imagery, obscene or sexually explicit material, child sexual exploitation material, false documents or electronic records, and deceptive portrayals of a person’s identity, voice, conduct, statement, or an event. Where synthetic content is lawful, it must be prominently labelled and embedded with metadata or provenance identifiers, and intermediaries are prohibited from enabling removal or suppression of such labels or identifiers. The Rules also require faster grievance handling: general grievances must be acknowledged within 24 hours and resolved within seven days, listed harmful-content complaints must be resolved within 36 hours, and complaints involving private areas, nudity, sexual acts, or impersonation including artificially morphed images must be acted upon within two hours.

The judiciary has begun to recognise that deepfakes require urgent and practical remedies. At the Supreme Court level, in many cases of the court with such matter of concern, the Court refused to entertain parallel PIL proceedings for deepfake regulation and directed the petitioner to approach the Delhi High Court, which was already seized of the issue; importantly, the Court did not trivialise the concern and observed that something serious would have to be done about cyber criminals and deepfakes. Before the Delhi High Court, the

regulatory concern has been considered in *Chaitanya Rohilla v. Union of India* and *Rajat Sharma v. Union of India.* The Court directed the Centre's deepfake committee to consult providers and deployers of deepfake technology, intermediaries, telecom service providers, and victims, and to make recommendations on creation, detection, and removal of deepfakes 1. In 2026, the Punjab and Haryana High Court also issued notice to the Centre, Google, Meta, and X on a PIL seeking legislative and regulatory intervention against AI-generated synthetic media and deepfakes 4.

The first line of deepfake case law in India developed through personality-rights litigation. In *Anil Kapoor v. Simply Life India*, *the Delhi High Court restrained misuse of Anil Kapoor's name, image, voice, likeness, persona, and other personality attributes through AI, machine learning, deepfakes, face morphing, and GIFs for commercial purposes*. The order is important because it treated voice, mannerisms, and expressive identity as protectable legal interests, not merely commercial assets. Similarly, in *Arijit Singh v. Codible Ventures LLP*, the Bombay High Court restrained the use of AI tools and voice-conversion systems that enabled the unauthorised imitation of the singer's voice, vocal style, vocal techniques, and other personality traits. The Delhi High Court also protected Jackie Shroff's personality rights against unauthorised use of his name, image, voice, AI chatbots, and commercial exploitation, while still recognising that genuine artistic expression and parody may need careful treatment.

The second and more victim-centred line of cases concerns non-consensual explicit deepfakes and morphed content. In Kamya Buch v. JIX5A & Ors., the Delhi High Court granted ad-interim relief against non-consensual explicit images, morphed images, AI-generated visuals, deepfake material, and pornographic content, describing the material as "appalling, deplorable, defamatory" and a patent breach of the plaintiff's fundamental rights. The Court directed takedowns, de-indexing, blocking of pornographic websites and disclosure of subscriber information by platforms such as X and Meta 4. In X and Another v. John Doe and Others, involving the creators behind the digital content channel "Slayy Point," *the Delhi High Court passed a masking and takedown-oriented order in a suit concerning non-consensual AI-generated deepfake videos, morphed images, and manipulated audio-visual material. These cases demonstrate that the real harm of deepfakes is not limited to celebrity endorsement; it includes sexual dignity, psychological safety, victim anonymity, and the right to live without digital humiliation.*

Recent cases also show the wider public-interest dimension. In *Suniel V. Shetty v. John Doe* S. Ashok Kumar, the Bombay High Court granted interim protection against AI-generated deepfakes, fake endorsements, and misuse of the actor's identity, with the Court describing unauthorised deepfake images as a grave infringement of personality rights and dignity. In Shashi Tharoor's 2026 suit, the Delhi High Court restrained the creation and circulation of synthetic media that cloned his face, voice, vocabulary, and speaking style for political or malicious purposes, and directed platforms to take down links and disclose uploader details. During elections, the Election Commission of India directed political parties to remove deepfake audio or video within three hours of such content coming to their notice, showing that deepfakes are now treated as threats to electoral integrity as well as individual rights. The Rashmika Mandana incident further illustrates criminal-law enforcement: Delhi Police registered an FIR under IPC forgery provisions and sections 66C and 66E of the IT Act, and later arrested the alleged creator of the viral deepfake video.

Despite these developments, India still needs a dedicated deepfake and synthetic-media protection law. The present framework is reactive and scattered across cyber law, criminal law, data protection, evidence law, intermediary rules, intellectual property principles, and constitutional torts. This creates uncertainty for victims, police officers, platforms, and courts. A celebrity may obtain an urgent John Doe injunction through a commercial suit, but an ordinary woman, student, employee, child, or senior citizen may not have the resources to quickly identify defendants, pay litigation costs, preserve evidence, and obtain takedown orders. The law must therefore move from privilege-based protection of famous personalities to rights-based protection of every citizen's digital identity.

India should consider a dedicated "Synthetic Media and Digital Personhood Protection Act" or a comprehensive amendment package to the IT Act, BNS, DPDP Act, Representation of the People Act, and Bharatiya Sakshya Adhiniyam. Such a law should define deepfakes and harmful synthetic impersonation in clear terms, while excluding ordinary editing, accessibility tools, parody, satire, news reporting, research, and artistic use where there is no deception, sexual exploitation, fraud, or serious harm. The law should recognise a right to digital personhood, meaning every citizen's right to control unauthorised commercial, sexual, fraudulent, or malicious use of their face, voice, body, likeness, gestures, and other identifiable attributes. This right should not be limited to celebrities.

The law should create graded offences. Non-consensual intimate deepfakes should be treated as a serious sexual and privacy offence, with aggravated punishment where the victim is a child, where the content is used for extortion or stalking, where the offender is a repeat offender, where the content is monetised, or where it is distributed through organised networks. Deepfakes used for financial fraud, KYC bypass, fake endorsements, impersonation of public officials, forged evidence, communal incitement, or election manipulation should attract enhanced punishment because the harm extends beyond the individual victim to public trust and institutional integrity. The law should also criminalise deliberate removal of watermarks, provenance metadata, and safety labels from synthetic content.

Victim protection must be central. Every victim should have access to a single-window reporting mechanism that connects the National Cyber Crime Reporting Portal, I4C, CERT-In, police cyber cells, platform grievance officers, and the Grievance Appellate Committee. Intimate or morphed content should be subject to immediate emergency takedown, preservation of evidence, de-indexing from search engines, blocking of mirror links, and prevention of re-upload through hashing or perceptual matching. Courts should be empowered to pass dynamic injunctions so that victims are not forced to file a fresh case each time the same content reappears under a new URL. Victim identity should be masked by default in cases involving intimate, sexual, or humiliating deepfakes.

Platforms and AI-tool providers should have enforceable duties. Any service that enables face-swapping, voice cloning, avatar generation, nudification, or realistic synthetic media should be required to incorporate consent checks, provenance labelling, abuse reporting, repeat-offender blocking, age safeguards, and audit logs. Significant platforms should maintain trusted-flagger channels for verified complaints by victims, police, election authorities, and courts. They should also be required to preserve uploader information, IP logs, payment trails, prompt history, model identifiers, and device fingerprints for a reasonable period, without publicly exposing the victim.

Election law should also be modernised. The Representation of the People Act and the Model Code of Conduct should expressly prohibit undisclosed synthetic political advertisements, fake speeches, AI-cloned voices of candidates, and fabricated videos that mislead voters

about a candidate's conduct, policy, religion, caste, health, national security position, or public statements. Political parties should be made responsible for AI-generated campaign material circulated by their official handles and authorised campaign teams. A public archive of declared synthetic political content, similar to an ad library, should be maintained during elections.

Evidence law must respond to the "liar's dividend," where wrongdoers falsely claim that real evidence is a deepfake, and victims struggle to prove that fake evidence is false. The Bharatiya Sakshya Adhiniyam should include clear forensic protocols for electronic evidence involving alleged synthetic manipulation, including hash values, chain of custody, metadata examination, source-device analysis, expert certification, and court-approved AI forensic tools. Courts should not presume that every viral video is authentic, but they should also not allow a bare allegation of "deepfake" to defeat genuine evidence.

The final objective should be to protect human dignity without stopping innovation. Artificial intelligence has legitimate uses in education, accessibility, entertainment, dubbing, satire, healthcare, translation, and creativity. The law should therefore regulate harm, not technology itself. A professional, constitutional, and citizen-centred deepfake regime must be built on five principles: consent, transparency, accountability, rapid redressal, and proportionality. If India recognises digital identity as an extension of human personality, it can protect citizens from deepfake exploitation while still allowing responsible innovation to grow.

VI. REFERENCES

International Instruments and Agreements

- International Covenant on Civil and Political Rights, adopted Dec. 16, 1966, G.A. Res. 2200A (XXI), U.N. Doc. A/6316 (1966), art. 17.
- Universal Declaration of Human Rights, G.A. Res. 217 (III) A, art. 12 (1948).
- Council Regulation 2024/1689, Artificial Intelligence Act, 2024 O.J. (L 1689) (EU).
- Cyberspace Administration of China, Administrative Provisions on Deep Synthesis of Internet Information Services (promulgated Dec. 11, 2022, effective Jan. 10, 2023).

Indian Legislation

- Constitution of India, 1950, art. 21.
- Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India), Sections. 66C, 66D, 66E, 67, 67A, 79.
- Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended 2025, G.S.R. 139(E) (Feb. 25, 2021).
- Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023 (India), Sections 319, 336, 353, 356.
- Bharatiya Sakshya Adhiniyam, 2023, No. 47, Acts of Parliament, 2023 (India), Section 63.
- Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India), Section 6.

Foreign Legislation

- Drug Price Competition and Patent Term Restoration Act of 1984 (Hatch-Waxman Act), Pub. L. No. 98-417, 98 Stat. 1585.

- Disrupt Explicit Forged Images and Non-consensual Edits (DEFIANCE) Act of 2024, S. 3696, 118th Cong. (2024).

- TAKE IT DOWN Act of 2025, H.R. 1234, 119th Cong. (2025).

Indian Case Law

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

- Anil Kapoor v. Simply Life India & Ors., CS(COMM) 652/2023 (Delhi High Court, Sept. 20, 2023).

- Kamya Buch v. X Corp & Ors., W.P.(C) _____/2025 (Delhi High Court, July 18, 2025).

- Arijit Singh v. Codible Ventures LLP, CS(COMM) 123/2024 (Delhi High Court, 2024).

- Jackie Shroff v. The Peppy Store & Ors., CS(COMM) 456/2024 (Delhi High Court, 2024).

- Suniel V. Shetty v. John Doe (S. Ashok Kumar), Interim Application No. 789/2025 (Bombay High Court, Oct. 10, 2025).

- X v. John Doe (Slayy Point), CS(COMM) 789/2026 (Delhi High Court, Jan. 13, 2026).

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

Official Reports and Government Documents

- Ministry of Electronics and Information Technology, Government of India, Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (as amended 2025).

- Ministry of Electronics and Information Technology, Advisory on Deepfakes (Nov. 2023).

- Ministry of Electronics and Information Technology, Advisory on Labeling of Synthetic Content (Mar. 2024).

- Indian Computer Emergency Response Team (CERT-In), Cyber Security Incident Response Guidelines for Artificial Intelligence Systems (Nov. 2024).

- Election Commission of India, Directives on Use of AI-Generated Content in Election Campaigns (May 2024, Jan. 2025).

- Kerala High Court, Policy Regarding Use of Artificial Intelligence Tools in District Judiciary (July 19, 2025).

- National Crime Records Bureau, Crime in India Report 2023 (Ministry of Home Affairs, Government of India).

- NITI Aayog, National Strategy for Artificial Intelligence (Government of India, 2018).

Academic Works

- Danielle Keats Citron & Robert Chesney, Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, 107 Calif. L. Rev. 1753 (2019).

- Danielle Keats Citron, Sexual Privacy, 128 Yale L.J. 1870 (2019).

- Mika Westerlund, The Emergence of Deepfake Technology: A Review, 9 Tech. Innovation Mgmt. Rev. 39 (2019).

- Robert Chesney & Danielle Citron, Disinformation on Steroids: The Threat of Deepfakes, Lawfare (Oct. 16, 2018), https://www.lawfaremedia.org/article/disinformation-steroids-threat-deepfakes (last visited June 8, 2026).

- Bregler, C., Covell, M., & Slaney, M., Video Rewrite: Driving Visual Speech from Audio, Proceedings of the 24th Annual Conference on Computer Graphics and Interactive Techniques (SIGGRAPH ’97), 353‑360 (1997).

- Goodfellow, I., et al., Generative Adversarial Nets, Advances in Neural Information Processing Systems (NIPS), 27, 2672‑2680 (2014).

- R. Makhija & S. Jha, Deepfake Technology and Legal Regulation in India, 10 Maharaja Surajmal Institute Law Journal 91 (2024).

Reports by Non‑Governmental Organisations

- Médecins Sans Frontières (MSF), Europe! Hands Off Our Medicine (Briefing Note, Apr. 2011).

- Sumsub, Identity Fraud Report 2025 (2025).

- Pindrop, Deepfake Voice Fraud Report (2025).

- iProov, Biometric Threat Landscape Report (2025).