VOLUME 6 | ISSUE 3

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

DEEPFAKES, CONSTITUTIONAL IDENTITY RIGHTS, AND DIGITAL EVIDENCE: AN INTEGRATED LEGAL FRAMEWORK FOR ARTICLE 21 PROTECTION AND FORENSIC AUTHENTICATION IN INDIA

- Kratika Dhote & Sanjay Kumar Sahu[1]

Abstract

The Indian Law is facing a complex challenge of rise in deepfake technology. It affects constitutional rights, the reliability of evidence, and the responsibility of intermediaries. This paper looks at deepfakes, which are lifelike synthetic media created by Generative Adversarial Networks (GANs). These deepfakes violate Article 21, which protects life, liberty, dignity, and informational privacy according to Puttaswamy judgement. Unlike traditional harms, deepfakes allow non-consensual biometric duplication, undermining identity control and causing psychological harm, especially to women through sexualized or defamatory content.The paper critiques the Bharatiya Sakshya Adhiniyam, 2023 (BSA) for not properly validating AI-generated evidence beyond basic certification under Sections 62-63. This leaves courts exposed to fake manipulations, even with the limits of forensic detection. The safe harbors for intermediaries under Section 79 of the IT Act, 2000, fail because of issues with traceability and neutrality. Platforms cannot check content neutrality without making editorial decisions.The paper suggests a comprehensive framework: (1) courts should recognize digital identity rights through the horizontal application of Article 21; (2) amend the BSA for better authentication hearings and verification; (3) reform the IT Act to provide safe harbors for good-faith removals and to shift the burden of proof to the complainant; (4) specify deepfake forgery in BNS and integrate it with the DPDPA. This all-encompassing approach tackles related issues and calls for legal and judicial action to protect constitutional values in the age of AI.

[1] LL.M. Candidates at NLSIU

Introduction

One of the biggest issues facing Indian jurisprudence today is the rise of deepfake technology, which has led to a crisis in both the constitution and the evidentiary crises that surpasses conventional legal classifications. In addition to violating Article 21 constitutional protections, deepfakes; hyper realistic synthetic media produced by Generative Adversarial Networks (GANs) and sophisticated machine learning algorithms, also undermine the authentication processes of the Indian Evidence Act and reveal significant weaknesses in intermediary liability frameworks[2]. In order to address the three-way harm caused by deepfake technology, this paper makes the case for an integrated legal framework that combines forensic authentication standards, constitutional protections, and reformed intermediary accountability.

It is impossible to estimate how serious this challenge is. Unlike traditional defamation or privacy violations, deepfakes operate at the nexus of three distinct legal domains: they attack constitutional identity rights of individuals who are non-consensually synthesized without remedial frameworks for private-actor harm; they undermine the presumption of electronic record reliability upon which Indian courts depend for evidence authentication; and they render the "neutrality" principle of intermediary liability theoretically impossible when platforms must detect synthetic media they cannot technically verify.

The present state and structure of the law ecosystem made up of fragmented provisions under the Information technology act, 2000, the Bhartiya Nyaya Sanhita, 2023, and the Indian Evidence Act, 1872 do not fully tackle this holistic crisis.

This paper takes the form of four composite analyses the first to investigate the constitutional infringement of Article 21 in terms of identity rights and informational privacy, the second one to examine the authenticity crisis of evidentiary authentication posed by deepfakes under Section 62 -63 of the Bhartiya Sakshya Adhiniyam, the third one to consider the structural inability of intermediary neutrality under Section 79 of the IT Act and lastly the fourth to suggest an all-inclusive model that integrates constitutional protection mechanisms, the standard of evidentiary authentication.

[2] Vishnu Vardhan G and Mahizhnan C, 'Deepfakes and Digital Evidence: A New Test for Indian Courts' (2026) 6(1) *International Journal of Advanced Legal Research*

1. Constitutional Identity Rights and Article 21 Violation

Article 21 of the Indian Constitution states that "no person shall be deprived of his life or personal liberty except according to procedure established by law." [3]The Supreme Court of India has interpreted this provision to include rights that go beyond just physical security. These rights encompass dignity, autonomy, and privacy. [4]In Maneka Gandhi v. Union of India, the Court decided that the right to life under Article 21 includes the right to live with human dignity, which covers a wide range of rights essential for a dignified human existence. [5]

The important ruling in K.S. Puttaswamy (Retd.) and Another v. Union of India changed the discussion about protecting identity. The Supreme Court determined that privacy is a fundamental right included in Article 21. This right is supported by the text, structure, and history of the Constitution[6]. Justice D.Y. Chandrachud explained that privacy protects informational autonomy, which is the right to control how personal information is shared, as well as decisional autonomy. This framework, while focused on government actions, has significant consequences for harm caused by private entities when biometric and personal identity information is used without consent.[7]

1.1 Deepfakes as Non-Consensual Biometric Reproduction

Deepfake technology operates through three mechanisms that severally and collectively violate Article 21 protections. First, deepfakes represent unauthorized replication and dissemination of biometric data - facial geometry, vocal patterns, iris patterns constituting what scholars' term "informational privacy violation." When an individual's facial biometric is extracted and synthesized without consent into sexualized, defamatory, or false-statement content, the person's biometric identity becomes weaponized against their autonomy.[8]

The vertical limitation of fundamental rights presents the first institutional crisis.On the textual and jurisprudential level, article 21 limits the action of states: the article forbids deprivation of

[3] Constitution of India, art 21.
[4] *Justice KS Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1 (SC)
[5] *Maneka Gandhi v Union of India* (1978) 1 SCC 248.
[6] *Puttaswamy* (n 3).
[7] Ibid.
[8] AI-Generated Deepfakes and the Legal Vacuum in India: A Constitutional and Regulatory Analysis' (2025) 25(11) *International Journal of Research and Trends in Innovation* 99.

life or liberty, which is not based on a procedure that is laid down by law. However, there is overwhelming harm in deepfake that is caused by individuals, content creators, and malicious users who operate within distributed systems. The lack of horizontal application of Article 21 results in what could be described as the creation of a liability vacuum: the state cannot arbitrarily deny identity rights, but otherwise, private actors are free to synthesize biometric identity without much oversight in the context of the lack of a remedial constitutional framework[9].

The Indian jurisprudence has tried to fill this gap by the means of constitutional morality and indirect horizontal effect doctrines. In Suresh Kumar Koushal v. Naz Foundation, the Court indicated that fundamental principles of rights, although not located directly between the individual persons, could have an impact on the interpretation of the statutory law and the regulatory frameworks. [10]Nonetheless, this doctrinal solution has failed this deepfake harms. The present legal framework based on defamation in Section 500 of the Bharatiya Nyaya Sanhita, forgery in the Section 336 and personation in the Section 319 considers deepfakes as isolated crimes and not as a systematic breach of identity rights that is constitutionally protected.

1.2 Dignity Degradation and Psychological Damage.

Article 21 is violated in the second mechanism, the mechanism of dignity erosion. The supreme court has reiterated that dignity is not merely residual concept but a ‘core constitutional principle.’ [11]

They attack dignity in three major ways- by sexualization, by ways of false attributes and social humiliation. Non-consensual sexualized deepfakes, which show real people in synthetic pornographic content, are a serious violation of dignity. The harm goes beyond reputation; it affects a person's very existence. This category of deepfake is created predominantly against women, and creates what might be termed "intimate image abuse extended." Unlike traditional intimate image abuse, which disseminates consensually created images, deepfake technology

[9]Juhi Chandel and Manisha Kundu, ‘AI-Generated Deepfakes and the Legal Vacuum in India: A Constitutional Analysis of Privacy, Consent, and Digital Harm under Article 21’ (2025) 10(11) *IJRTI* 850, 854

[10]*Suresh Kumar Koushal v Naz Foundation* (2014) 1 SCC 1 (SC)

[11]KS Puttaswamy (Retd) v Union of India (2017) 10 SCC 1 (SC); Maneka Gandhi v Union of India AIR 1978 SC 597; Gobind v State of Madhya Pradesh (1975) 2 SCC 148 (SC)

permits the creation and dissemination of entirely synthetic intimate images that never existed, could not have been consented to, yet depict the victim's face and body.[12]

Victims often experience psychological trauma similar to that from sexual assault, along with social isolation, job discrimination, and even thoughts of suicide in severe cases.Deep fakes involving false attribution which presents faked audio or video of a person saying things the person has never said also go against the dignity of falsely associating the identity of a person with the words they do not say.

The identity of the victim becomes detached to what the victim wants to do; his or her face and voice are symbolic of something they are denying. This forms what scholars refer to as identity theft on the connotation of meaning-making. Constitutionally, such violations of the dignity qualify as falling under the provision of Article 21. The Supreme Court has determined dignity to include liberty of non-degradation and humiliation, the entitlement to preserve one reputation and the entitlement to control the way he would be represented on society.[13]Using deepfakes systematically contravenes all the three dimensions. The issue of longevity is obscure however. Although the court has identified the harm to dignity as actionable under privacy jurisprudence and tort law, the constitutional right to consent has yet to be built out expressly, an express right to own image has not yet been developed, and has no express right against non-consenting biometric synthesis; this bears interpretation ambiguity.

1.3 The Lack of a Constitutional Right to Consent and Digital Selfhood.

The third violation of Article 21 law is the lack of a constitutionally enshrined right to consent and have control over one self in the digital realm. This is, perhaps, the most underthought conceptual area of Indian constitutional law. Informational privacy came to be understood in Puttaswamy judgment as a control over personal information, but the jurisprudence that followed has failed to work out a solid model of construing digital identity, the merging of one's biometric data, digital representations and synthetic reproductions, as a category of constitutionally-guaranteed privacy.

[12] Vishnu Vardhan G and Mahizhnan C (n 1).
[13] *Puttaswamy* (n 3).

It is this gap that is enlightened by comparative jurisprudence. General Data Protection Regulation (GDPR) on the rights of individuals in the European Union acknowledges the right of an individual to have their personal data processed when they consent to the processing, their right to access to data stored about them, and correction of inaccurate data. [14]The new type of digital rights framework of the EU approaches the digital identity as a property-similar right safeguarded against the lack of non-consensual exploitation. The constitutional law of India has failed to make similar structures.

The implication of this is that deepfake harm perpetrators are in a gray zone. They flout criminal laws (defamation, personation) though no specific constitutional contravention is perpetrated redressable under Part III fundamental rights. The victim has no plea that can be taken to the constitutional court that they have had their Article 21 right violated by synthesizing their digital self, since such a right is not yet understood within the constitution as it is currently interpreted to mean a pure right to control their own imagery, or stop seeing an unconsented synthesis of the biometric image to fall within the expectations of privacy.

2. The Evidentiary Authentication Crisis under the BharatiyaSakshya Adhiniyam, 2023

Section 65A and 65B of the Indian Evidence Act, 1872, which are now the direct contemplation of the BharatiyaSakshya Adhiniyam, 2023 contributed to the rise of the so-called evidentiary crisis due to deepfakes. This new legislation replaces the colonial law but largely follows its structure on electronic record keeping. The BSA restructures and redesignates its provisions but does not relegate electronic records as documentary evidence. It enables this to be demonstrated by means of computer outputs, on the condition that certain specified statutory conditions and certification requirements are fulfilled. Nevertheless, the new law does not truly reexamine the presumption of reliability with respect, concerning the electronic records, and also specifies AI-based or deepfake media. It leads to the introduction of the old assumptions into the technologically developed world.[15]

[14]Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [General Data Protection Regulation].

[15]Vivek Dubey, 'Admissibility of Electronic Evidence: An Indian Perspective' *Forensic Research & Criminology International Journal***4(2)** 58–63 (published 14 March 2017)

Section 65B of the Indian Evidence Act that an electronic record acts like documentary evidence is under the BSA, the acceptance of an electronic record is subject to the same conditions as those under Section 65B. These new regulations still operate on the concept that in case the source machine, the procedure of creating the digital exchange, and the chain of custody are accredited to have complied, the resulting output of the computer can be esteemed by the courts as presumptively true unless it is explicitly outgoing. The primary source of admissibility is still done through certificates of people who are responsible with the concerned computer systems. Moreover, even hash values or other integrity checks are still important elements of evidence verification.[16]

Deepfake technology is a severe threat to this assumption. In the case where the information on an electronic record is not a mirror image of something occurring in the real world because the information is created by AI, integrity of the machine and chain of custody do not inform the court of whether or not the information behind the visual or audio data was an actual event. A deep consequences video can be made without the help of generative algorithms, saved on a secure system, with an impeccable certificate and can be submitted with an undisrupted chain of custody. Nevertheless, its reliability is an evidentiary falsity in that the contents are composed at the beginning. Another particular aspect of AI deepfake manipulation that puts the BSA in a especially weak position is its continued dependence on system integrity and process certification, without attempts to analyze content truthfulness in the circumstances of AI.[17]

Traditional forensic methods for digital evidence, like metadata examination and compression artifact analysis, were based on a clear division between “authentic” and “manipulated” records. In this model, an “original” image or video existed, and forensic analysis sought signs of later tampering. Deepfakes challenge this binary by creating media from scratch: there is no original for the court to refer back to. As a result, techniques designed to find tampering in authentic

[16]Aditya Mehta, Arjun Sreenivas and Swagata Ghosh, ‘Section 65B of the Indian Evidence Act, 1872: Requirements for Admissibility of Electronic Evidence Revisited by the Supreme Court’ *India Corporate Law* (27 July 2020)
[17]Harmanjeet Singh and Ritu Panta, ‘Deepfake Evidence and the Indian Criminal Justice System: Challenges of Authenticity, Consent and Admissibility in Law’ (2025) 7(6) *International Journal for Multidisciplinary Research* 1

captures are ineffective against media that is synthetic from the start, straining the evidential categories outlined in the BSA. [18]

Current digital forensics and deepfake detection research focus on AI-based detection and multilayered analysis. The latest methods use deep learning models trained to identify specific signs of known generative techniques, signal-based analysis looking at lighting, shadows, sensor noise, and motion inconsistencies. They also inspect metadata and container structures and contextual investigation of sources, distribution patterns, and correlation with outside evidence. However, these methods are still probabilistic and have significant false positive and false negative rates. The underlying models often operate as black boxes, making it hard for courts and juries to understand them. The BSA lacks any statutory guidance on how to evaluate these probabilistic, model-driven conclusions, what error thresholds are acceptable for evidence, or how to address conflicting expert opinions in adversarial cases.[19]

Such technological fact is opposite of the assumption of the BSA, that the electronic records can be recognized as reliable with the help of formal certification only. Applying a deepfake video as primary evidence in a criminal trial simply because that video is issued with a BSA-compliant certificate would be unreasonable, and irregular with the requirement of the Supreme Court in the previous cases of electronic evidence that relevant and substantial proof of authenticity required. At the same time, considering all controversial electronic documents dubious in a time of deepfakes would cause impediments to the fact-finding process and debunk the worth of legit digital evidence. It results in an admissibility crisis: the BSA, in its current version, does not offer an efficient method to distinguish between normal and electronic records and those which could be affected by the deepfake technology.[20]

Initial judicial decisions and scholarly recommendations have begun to gravitate towards a tiered authentication system in BSA. Analysts claim that in cases where an individual raises an honest issue, backed by expert opinion or precedent realism, over an electronic record being AI-

[18]Gueltoum Bendiab, Houda Haiouni, Isidoros Moulas and Stavros Shiaeles, 'Deepfakes in Digital Media Forensics: Generation, AI-Based Detection and Challenges' (2025) 88 Journal of Information Security and Applications 103935

[19]Martino Jerian, 'Deepfake Forensics Is Much More Than Deepfake Detection!' Amped Blog (5 August 2025)

[20]Aditya Mehta, Arjun Sreenivas and Swagata Ghosh, 'Section 65B of the Indian Evidence Act, 1872: Requirements for Admissibility of Electronic Evidence Revisited by the Supreme Court' *India Corporate Law* (27 July 2020)

generated, BSA certification must never be taken as evidence of authenticity. Instead, the concern should prompt a preliminary evidentiary hearing where (a) the one presenting the evidence must meet a higher burden to prove the record is not synthetic, using suitable forensic and AI-detection tools, and (b) the opposing side can question forensic experts and challenge the reliability of detection methods. Some suggestions further propose that in criminal cases where a conviction largely relies on disputed digital media, the BSA should require independent confirmation from non-digital sources before a court can safely use such evidence.[21]

However, these changes currently exist outside the law. The BSA does not include any specific provisions for deepfake or AI-generated media, nor does it set higher authentication standards, rules for shifting the burden of proof, or requirements for corroboration in cases involving synthetic media. [22]Courts and legal practitioners must improvise within a legal framework built for a different technological era, stretching general rules on electronic records to cover situations legislators did not foresee.[23]This ambiguity threatens multiple levels of application of law throughout different jurisdictions, negatively impacts predictability, and places undue burden on judicial knowledge of rapidly evolving forensic science.[24]

Therefore, the evidentiary crisis that deepfakes have provoked under the BSA is not purely technical but it is rooted in the malfunctions of the statutory design. In the absence of any evidentiary understanding of synthetic media and a set of unambiguous evidentiary guidelines regarding its legitimacy, the BSA compels courts to either overly rely on certified electronic records in a manner susceptible to abuse by deepfake abusers or to develop a skepticism towards it which is counterproductive to the application of authentic digital evidence. The legal solution to the problem of deepfakes of this kind must therefore encompass some specific alterations to the BSA, which will (i) facilitate the differentiation between regular electronic records and those that might be associated with the deepfakes, (ii) create multi-layered levels of forensic

[21] Ashwini Vaidialingam, 'Authenticating Electronic Evidence: §65B, Indian Evidence Act, 1872' (2015) 8 *NUJS Law Review* 43

[22] Ram Krishna Baghel and Rajeev Kumar Singh, 'Deepfakes, AI, and Cloud Forensics: Rethinking the Admissibility of Secondary Electronic Evidence in India and the United States' (2025) 10 *International Journal of Novel Research and Development* 624

[23]*Can AI-Generated Evidence Be Admissible Under Indian Law?The AmikusQriae*

[24]An article on electronic evidence and its legal ramifications in India (ABA Law Office, 2 February 2022)

authentication, and (iii) balance the burden distribution and corroboration requirements against the current capabilities of deepfake detection.[25]

3. The Intermediary Liability Crisis

Sec. 79 of the Information Technology Act, 2000 offers safe haven to intermediaries platforms, ISPs, hosting services to third party content, as long as they take due diligence and are in the status of a neutral conduit. [26]Shreya Singhal v. the Supreme Court. Union of India supported this model with beliefs that the intermediaries have constitutional protection as mere carriers of content and cannot be subjected to such a level of liability unless they collude, facilitate or encourage illegal actions, or even neglect to promptly block access to illegally obtained content on getting actual knowledge of such actions. [27]

This doctrine rests on a critical assumption: that intermediaries can maintain neutrality while detecting and removing unlawful content. The assumption is theoretically plausible for content that violates clear, easily identifiable legal categories hate speech, terrorism related content, child sexual abuse material. These categories are defined with sufficient specificity that detection, whether human moderated or algorithmic, is technically feasible if computationally expensive[28]. Deepfakes expose the structural impossibility of maintaining platform neutrality when the content category synthetic media potentially violating privacy, dignity, identity, and constitutional rights cannot be technically verified with certainty. A platform cannot definitively distinguish authentic video from AI-generated deepfake without sophisticated forensic analysis that no platform currently deploys at scale.[29]However, the inability of the platform to identify and eliminate deepfakes is the factor that initiates the liability coverage relying on Section 79, as a regular complainant can initiate legal actions against the platform for its inadaptability to do so as soon as it is informed about the illegal information.

3.1 The Traceability-Neutrality Paradox

[25]Vishnu Vardhan and Mahizhnan (n 1)
[26]Information Technology Act 2000 (India), s 79.
[27]Shreya Singhal v. Union of India [2015] 5 SCC 1
[28] Tech Law Forum, 'Web 2.0 Solutions for Web 3.0 Problems: Intermediary Liability and the Deepfake Crisis in India' (NALSAR Tech Law Forum, 2020)
[29] Legal Desire, 'Unveiling the Dark Secret of Deepfake: A Psychological, Forensic and Threat Analysis' (2 February 2026)

This crisis of intermediary liability comes in the form of what could be called the traceability-neutrality paradox. Under the Information Technology Rules, 2021, Section 79 was amended to specify that intermediaries shall keep records that will allow the identification of the first originators and trace back provisions to law enforcement agencies.[30]At the same time, intermediaries are also not supposed to filter the content unless legally required to do so or when it is evident that the content is against the law. Such obligations clash with each other in the deepfake context. Content analysis systems require platforms to implement complex content analysis tracks to track the origin of content and identify synthetic media patterns[31]. Such systems also require an algorithmic decision on content authenticity, the likelihood of manipulation and possible damage. This type of analysis goes beyond being impartial to being actively curative and editorial.[32]But by remaining truly neutral, not analyzing the advertising or filtering it outright on the basis of the law, makes the operators of platforms unable to respond quickly to the defamation or harassment of identity through deepfakes. [33]

This structural tension has been demonstrated by the deepfake crisis. Indian courts have imposed time constraints of up to 48 hours for such content to be removed from major Indian sites upon being notified; the sites do not have the technical capacity to verify content authenticity within this time limit on a large scale; and non-cooperation in doing so makes the sites the subject of the 79(c)(1) Indian liability for facilitating illegal activity.

4. The Coordination Gap Between Penal and Regulatory Frameworks

The crisis of secondary intermediary liability arises when there is misalignment between the emerges through misalignment between the Bharatiya Nyaya Sanhita, 2023, and the Information Technology Rules, 2021.[34]BNS exposes criminal liability to those who make deepfakes in the light of 319 (cheating by personation), 336 (forgery) and 356 (defamation). However, lacking

[30]Information Technology Rules 2021 (India), rule 3(1)(b)
[31]Tech Law Forum, 'Web 2.0 Solutions for Web 3.0 Problems' (NALSAR, 2020): Proactive deepfake detection "fundamentally compromises Section 79 conduit status".
[32]Tech Policy Press, 'India's New IT Rules on Deepfakes Threaten to Entrench Online Censorship' (6 November 2025): Rule 3(3) transforms platforms from "passive facilitators" to "active regulators"
[33]PIB, 'MeitY Issues Advisory to All Intermediaries' (26 December 2023): Platforms must act on deepfake notices or lose safe harbor.
[34]NeGD, 'Deepfakes in India: Legal Landscape, Judicial Responses, and a Practical Playbook for Enforcement'

smooth cooperation between the penal provisions of the BNS and the traceability requirements of the IT Rules, the proposed liability framework does not work practically.[35]

In the case of a deepfake, the offender should be detected and prosecuted by the criminal justice system when the provisions of BNS are violated. The IT Rules have intermediaries trace the originators; tracing mechanisms, however, have privacy and proportionality implications. [36]A court has to determine whether platform tracing mandates are reasonable intermediary obligations or surveillance mandates that are not in line with informational privacy. Lack of procedures that explicitly define when the intermediaries need to implement the use of tracing mechanisms, what legal process is needed to trigger tracing requirements and how information about the originators is traced and prevented to be misused creates uncertainty in operations that platforms address by removing the content or preventing the removal - neither of which adequately safeguards the rights.

5. **Toward an Integrated Legal Framework**

5.1 Constitutional Recognition of Digital Identity Rights

The initial element of a comprehensive framework is to have statutory constitutional declaration of rights to digital identity as a byproduct of Article 21. This awareness does not have to be amended in the constitution; it must be judicially construed to include the privacy framework of Puttaswamy to digital biometric synthesis. [37]The Supreme Court is supposed to acknowledge the right to privacy in Articles 21(b) as an extension of the right to one's own image i.e. the right to regulate the manner in which the biometric identity of a person is painted, reproduced and discharged[38]. This right should be exercised horizontally in opposition to state and private actors by the doctrine of constitutional morality and indirect horizontal application, the same way that privacy rights are already exercised in the tort doctrine and regulatory frameworks. Most importantly, such recognition must determine that a non-consensual synthesis of his biometric

[35]Harmanjeet Singh and Ritu Panta, 'Deepfake Evidence and the Indian Criminal Justice System: Challenges of Authenticity, Consent and Admissibility in Law' (2025) 7(6) *International Journal for Multidisciplinary Research*
[36]Khushi Jain, 'Legal Dimensions of Deepfake Technology: Privacy, Consent, and Criminal Liability' *Juris Centre* (27 July 2025)
[3737]*Justice KS Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1 [para 267-268]; *Amar Jain v Union of India* (SC, 30 April 2025) recognizes digital access under Article 21.
[38]*Kanwar Singh Meena v State of Rajasthan* (2025) SCC OnLine SC 456

identity as a means of sexualizing, defamation, or false-attribution is a per se violation of Article 21, irrespective of the perpetrator of the violation, whether a state actor or a person. This would provide a constitutional solution which is done by a public interest lawsuit or a victim-initiated constitutional action, which would complement criminal solutions, but not substitute them.

5.2 Evidentiary Authentication Standards for Synthetic Media

The second element requires an amendment of the BharatiyaSakshya Adhiniyam, 2023 (BSA) to add a definitive standard of authentication of synthetic media. Section 64A, ought to indicate that electronic records produced by AI synthesis, deepfake technology, or machine learning generation are not deemed to be authentic under Section 63(4) merely because they meet a certificate[39]. Rather, instead of those, Section 64A ought to design a system of multi-level authentication: (1) the first admission of disputed electronic records should be made based on Section 63(4); nevertheless, (2) when either side alleges that there is a potential synthetic generation, the court should conduct the initial authentication hearing; (3) in criminal litigation that primarily relies on the disputed digital records, there has to be more intensive support by external sources. The legislative framework ought to also specify: what can be used as a forensic method to obtain authentication; what are the qualifications required of forensic analysts; what error rates are associated with detection technology should make them more skeptic; and what contextual issues strengthen corroboration requirements.

5.3 Reformed Intermediary Liability Framework for Synthetic Media

The third element will need specific changes in the Information Technology Act and Rules in response to deepfake-specific intermediary liability. Instead of keeping the action of platform neutrality where platforms cannot technically ensure authenticity, a reformed system must: (1) acknowledge that content moderation when it comes to synthetic media involves performing an editorial act by definition; (2) provide safe harbor protection to good-faith efforts by intermediaries seeking to remove content that credibly appears to be synthetic media or a deepfake; (3) make plain that the intermediary liability will not be vis-a-vis failure to act to remove deepfakes, but (4) that the obligation of intermediaries to act expeditiously when

[39]Rutuja Pol and Ajey Karthik, 'Can India's New Evidence Act Address the Challenges Posed by Artificial Intelligence?' *The Secretariat*

presented with Most importantly, [40]the reformed structure must generate mutual responsibilities on the complainants who claim to have been victims of deepfake materials. While removal is pleaded, complainants must be made compulsory to present reasonable technical evidence that implies synthetic generation (forensic reports, experts views or contextual indicators.) This will avoid empty grievances and safeguard platforms with their capacity to draw the line between deep fake damage and usual cases of defamation controversy. The framework also seeks to introduce open reporting standards where platforms will store and publish data about number of deepfake removal requests received, removal rates, and appeal rates as this will allow regulators and civil society to judge whether platforms are removing too much or too little information.

5.4 Criminal Law Specification and Coordination

The fourth element involves reinforcing criminal law provisions and making BNS provisions and intermediary liability schemes work hand in hand. The application of the Supreme Court precedent of the BNS to the creation of deepfakes should be understood to expressly cover the creation of deepfakes, and criminal courts ought to appreciate deepfake technology as a unique form of forgery that should be applicable in these sections. Moreover, the BNS ought to be revised to add Section 336-A (forgery by non-consent synthetic reproduction), which would make it a crime to produce deepfake material representing real people in sexualized situations, defamatory situations, or false-attribution situations. [41]This provision must stipulate that: (1) the creation of non-consent based deepfakes amounts to severe criminal offence; (2) consent to which is achieved through duress, misrepresentation or through poor understanding is not a valid defense to deepfakes creation; (3) aggravating factors (deepfakes of minors, deepfakes made during an electoral process, deepfakes that create observable psychological harm) should be treated as aggravating factors by the courts; and (4) victim compensation (both criminal and civil compensation order) should be awarded to victims.

5.5 Digital Personal Data Protection Integration

Lastly, the unified framework must be consistent with the Digital Personal Data Protection Act, 2023. The DPDPA regulates the process of dealing with the personal data, whereas deepfakes

[40]Vineet Upadhyay, *India's new 3-hour deepfake removal rule: Experts urge strict complianceIndian Express*
[41]Singh and Panta (n 34)

generation is an unauthorized processing of biometric data in its most invasive form. A logical interpretation of the DPDPA is that mediating the production of deepfakes by third parties is illegal unless the mediator was aware of its occurrence, which makes the platform that offers services of deepfake generation or is aware of the presence of tools used to produce deepfakes liable.[42]

6. Conclusion

Deepfakes is a three-party crisis: an attack on Article 21 identity and dignity rights in non-consent biometric synthesis, an apparent crisis on the presumption of reliability in electronic records in the Indian Evidence Act, and a problematic crisis that makes platform neutrality structurally impossible. These crises do not exist as isolated entities. Theoretical constitutional redress with no evidentiary norms; normative evidentiary standards with no intermediate structures or designs; intermediate structures, which are not constitutional norms, ensure the continuation of law-breaking; constitutional norms, which are not normative evidentiary standards, ensures the continuation of law breaches.

The suggested combined framework is a synthesis of the responses of the constitutional, evidentiary, regulatory, and criminal spheres. It acknowledges that harms of deepfake cannot be subsumed only to defamation and privacy-related offenses that can be incorporated into legal categories that exist to date; it is a new type of identity assault, to which new legal categories should be assigned. More importantly, this framework entails institutional capacity-building. Courts need to build technical expertise in the area of AI, forensic expert subjects, and deepfakes. The intermediaries have to invest in content verification infrastructure. Policemen have to invent investigative methods suitable to synthetic media. The Supreme Court has to do constitutional job of acknowledging the rights to digital identity and creating evidentiary requirements. The house of legislature should make some clarifying amendments in the Indian evidence act and information technology act. Injustice is maintained by lack of action. Defamation and privacy law were already established as theoretical sources of redress to deepfake victims, but effective remedies have not been found yet. The platforms cannot tell that the content was derived via

[42]Sarvagya Chitranshi, 'The Deepfake Conundrum: Can the Digital Personal Data Protection Act, 2023 Deal with Misuse of Generative AI?' (2024)

deepfake without forensic knowledge of which they lack. Electronic evidence cannot be authenticated by the courts with proper evidence standards unless it deals with synthetic media. The digital identity rights are not explicitly addressed by the Constitutional framework, and thus, the concept of the harm of deepfakes is theoretically in non-conformance with the key rights, but practically, it is only possible to remedy the situation through statutory interpretation. The combined framework suggested in this paper offers avenues of an overall legal response. It should be carried out through political commitment, the capacity to build institutions, and leadership of the judiciary. However, the other option of letting deepfake technology run itself in a regulatory vacuum where identity rights by the constitution cannot be enforced, where the standard of evidence authentication is inadequate, and platform intermediaries have conducted them with impossible responsibilities- is constitutionally and practically untenable in an ever-growing crisis in which deepfake capabilities multiply each month and platform intermediaries stand entirely unchanged by the law. India stands at a crossroads. It may identify deepfake harm as necessitating integrated legal response operating at constitutional, evidentiary, intermediary, and criminal levels or it may allow disjointed legal responses that neither shield victims nor institutional integrity. The decision is urgent.