JOURNAL OF CYBER GOVERNANCE AND INTELLECTUAL PROPERTY

Volume 1, Issue 2 Article 5

Regulating Synthetic Identity: Protecting Ordinary Citizens against Deepfake Impersonation in India

Aakanksha Nigam

Kishinchand Chellaram Law College, University of Mumbai

Recommended Citation:

Nigam (2026) "Regulating Synthetic Identity: Protecting Ordinary Citizens against Deepfake Impersonation in India" Journal of Cyber Governance and Intellectual Property, Vol. 1, Issue 2, Article 5. (DOI)

ABSTRACT

The widespread adoption of Generative AI in 2022 challenged the long standing assumptions about the authenticity of digital identity by making it possible to create highly convincing synthetic media using readily available AI tools. As a result, deepfake impersonation now threatens personal security, economic interests, social standing, and legal rights, exposing the limitations of existing laws in protecting identity and digital authenticity. This paper examines the adequacy of India's existing legal framework in addressing deepfake impersonation affecting ordinary citizens through an analysis of constitutional principles, statutory law, judicial decisions, and recent regulatory developments. It argues that the current framework is predominantly reactive and consequence based, relying on sector specific remedies that struggle to address AI generated impersonation itself as a distinct legal harm. The paper further evaluates gaps in personality rights, data protection, evidentiary standards, and intermediary responsibility. It concludes that the absence of a coherent legal framework with respect to deepfake impersonation leaves ordinary citizens of India reliant on fragmented remedies after harm has occurred because AI generated impersonation remains unrecognised as a distinct legal harm.

KEYWORDS

Deepfakes, Citizens, Digital Authenticity, Article 21, Personality Rights, Evidence Law, AI Governance, India.

INTRODUCTION

For generations, digital records including photographs, recorded voices, and videos were widely treated as reliable evidence of identity both in everyday interaction as well as the legal system. Courts relied on recorded evidence, employers trusted digital communication, and individuals shared their lives online with the expectation that their identity remained their own. However, the rapid proliferation of deepfake technology has shattered this trust, as it continues to produce highly realistic images, videos, and voice recordings that imitate a person with remarkable accuracy.

Deepfake impersonation has impacted not only the celebrities or political figures, but also ordinary citizens who are increasingly becoming its victims. According to 2025 analysis of Artificial intelligence scam through the unauthorised use of photographs, voice recordings, and other identifying characteristics available on digital platforms has recorded that 47 percent of adults are victims or know someone who has been a victim of deepfake impersonation.[1] These synthetic impersonations have emerged as a proven tactic for cybercrime enabling financial fraud, executive impersonation, identity theft, and disinformation campaigns and have therefore expanded the legal debate beyond technological misuse to questions concerning personality rights, informational privacy, and the protection of individual dignity. While Indian law does not expressly recognise personality rights through a single statute, judicial decisions have derived such protection from the constitutional guarantee of privacy under Article 21, as recognised in Justice K.S. Puttaswamy (Retd.) v. Union of India.[2] While the judiciary has shown agility in responding to these individual violations, India's formal legal architecture addresses such harms through a patchwork of existing laws rather than a singular, dedicated statute. Article 21 of the Constitution protects privacy, dignity, and personal autonomy, while Article 19(2) permits reasonable restrictions on speech where expression infringes the rights or reputation of others. Statutory protection is dispersed across the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Bharatiya Sakshya Adhiniyam, 2023, the Digital Personal Data Protection Act, 2023, and the Information Technology (Intermediary Guidelines and Digital

[1] Pranoy Jainendran, Deepfakes and Financial Cybercrime: India's Multi-Layered Response, OBSERVER RESEARCH FOUNDATION (Jan. 15, 2026), https://www.orfonline.org/expert-speak/deepfakes-and-financial-cybercrime-india-s-multi-layered-response (last visited July 28, 2026).

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

Media Ethics Code) Rules, 2021 and more recently, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, which introduced additional obligations concerning AI generated synthetic content, including enhanced due diligence, traceability, and expedited action against unlawful content generated through artificial intelligence. Even though these measures reflect a growing regulatory recognition of the risks posed by deepfakes, India's legal response remains scattered across multiple statutes and regulatory instruments that were not originally enacted to address AI enabled identity manipulation. Consequently, the present legal framework is better suited to addressing the aftermath of deepfake exploitation since it is rather reactive than preventive in nature.

LITERATURE REVIEW

The emergence of Generative AI has redefined the legal discourse on deepfake technology. While early discussions primarily focused on the technical development of artificial intelligence, the increasing accessibility of Generative AI has redirected the attention of the scholars towards the impact of AI enabled impersonation on ordinary individuals. Deepfakes are generally understood as synthetic media created through machine learning models, particularly Generative Adversarial Networks (GANs), which are capable of producing highly realistic images, audio recordings, and videos.[3] Unlike conventional photo or video editing, these systems generate entirely new digital content that closely replicates an individual's appearance or voice and are hyper-realistic. Consequently, concerns surrounding deepfakes now extend beyond misinformation to encompass privacy, reputation, personal autonomy, identity theft, financial fraud, and non-consensual exploitation, particularly where fabricated content becomes indistinguishable from authentic recordings.[4]

The practical implications of this shift became evident when Meta introduced an AI image-generation feature on 7 July 2026. This Instagram tagging feature allowed users to generate AI images using publicly available Instagram photographs of others.[5] However, following intense criticism from privacy advocates and unions such as SAG-AFTRA regarding

[3] Prakash L. Kharvi, *Understanding the Impact of AI-Generated Deepfakes on Public Opinion, Political Discourse, and Personal Security in Social Media*, IEEE SEC. & PRIV., July/Aug. 2024.
[4] Kharvi, supra note 3.
[5] Kevin Collier, *Meta's AI Is Being Used to Create Deepfakes of Real People on Instagram*, NBC NEWS (July 17, 2024, 3:30 AM EDT), https://www.nbcnews.com/tech/social-media/meta-ai-muse-instagram-deepfakes-rcna353480. (last visited July 28, 2026).

the tool's capacity for creating non-consensual deepfakes, it was withdrawn just three days later.[6] These developments reinforce Kharvi's observation that deepfake technology poses an "epistemic threat" by enabling the creation of material that is "nearly indistinguishable from authentic material," thereby increasing the likelihood that individuals will acquire false beliefs and challenging conventional assumptions of truth and authenticity in the digital environment.[7]

Scholarly analysis further indicates that India's existing statutory framework provides only partial protection against harms arising from deepfake technology. The Information Technology Act, 2000 penalizes digital offenses through distinct provisions: Section 66C addresses identity theft, Section 66D prohibits cheating by impersonation, Section 66E protects against privacy violations, and Section 67 outlaws the publication of obscene electronic material.[8] Similarly, the Bharatiya Nyaya Sanhita, 2023 addresses offences including cheating, forgery, defamation, and offences affecting reputation[9], while the Digital Personal Data Protection Act, 2023 establishes a consent-based regime governing the processing of digital personal data.[10] Nevertheless, several scholars contend that these enactments primarily address the aftermath of deepfake misuse rather than regulating the creation, dissemination, or misuse of manipulated media itself. Concerns have also been expressed regarding the absence of clear statutory safeguards governing the use of publicly available biometric data, including facial images and voice samples, for training artificial intelligence systems without genuine consent.[11]

Recent literature also reflects a gradual movement towards greater intermediary accountability. Amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules have strengthened the obligations of digital intermediaries by enhanced due diligence relating to AI generated content and platform governance.[12] Even though these measures represent an important regulatory development, commentators have observed that their effectiveness eventually depends upon institutional capacity, timely enforcement, and the

[6] *Why Has Meta Pulled Back Muse AI Feature from Instagram?*, THE HINDU (July 18, 2024), https://www.thehindu.com/sci-tech/technology/why-has-meta-pulled-back-muse-ai-feature-from-instagram/article71215966.ece (last visited July 28, 2026).
[7] Kharvi, supra note 3.
[8] Information Technology Act, 2000, §§ 66C, 66D, 66E, 67, No. 21, Acts of Parliament, 2000 (India).
[9] Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023 (India).
[10] Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
[11] Juhi Chandel & Manisha Kundu, *AI-Generated Deepfakes and the Legal Vacuum in India: A Constitutional Analysis of Privacy, Consent, and Digital Harm Under Article 21*, 10 INT'L J. RSCH. TRENDS & INNOVATION 1, 10, 15–16 (2025).
[12] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E), Gazette of India, Extraordinary, pt. II, sec. 3(i), Feb. 25, 2021 (as amended Feb. 10, 2026).

availability of technical expertise within investigative agencies, digital forensic laboratories, and the judiciary.[13] An additional prominent theme emerging from the literature concerns the impact of deepfakes on the law of electronic evidence. Traditional evidentiary principles assumed that digital multimedia could be authenticated solely through forensic verification. For instance, under Section 63 of the Bharatiya Sakshya Adhiniyam, 2023, any digital media presented as electronic evidence must now satisfy strict, mandatory statutory certification and hash-value profiling before it can be admitted as evidence.[14] However, with the widespread adoption of Generative AI, scholars have begun to question whether these assumptions remain adequate when artificial intelligence can generate fabricated content that is visually and audibly indistinguishable from genuine recordings.

The consensus across the literature is that the mere possibility of hyperrealistic deepfakes has precipitated a "crisis of evidence" within legal and institutional frameworks[15]. Scholars further argue that this development has complicated judicial decision-making by enabling parties to cast doubt on the authenticity of genuine digital evidence, a phenomenon commonly described as the "Liar's Dividend."[16] Consequently, courts may no longer accept audiovisual records at face value and instead require additional forensic verification and corroborative evidence, thereby increasing the cost, complexity, and duration of legal proceedings while placing greater demands on the judiciary and litigants. The researchers further identify continuing deficiencies in India's digital forensic infrastructure, including limited technical expertise, inconsistent forensic standards, and inadequate detection capabilities for sophisticated AI generated content.[17]

Additionally, the scholars have identified a critical "horizontal vacuum", recognising that fundamental rights primarily regulate the relationship between the State and the individual, whereas most deepfake related harms are inflicted by private actors operating through digital platforms.[18] This limitation, when coupled with the fragmented and reactive nature of India's existing legal framework, prompts growing scholars to support for a comprehensive statutory

[13] Harmanjeet Singh & Ritu Panta, *Deepfake Evidence and the Indian Criminal Justice System: Challenges of Authenticity, Consent and Admissibility in Law*, 7 INT'L J. MULTIDISCIPLINARY RSCH. 1, 18–20 (2025); Supra note 11.
[14] Bharatiya Sakshya Adhiniyam, 2023, § 63, No. 47, Acts of Parliament, 2023 (India).
[15] Abhishek Kukreti, Vivek Kumar & Avishek Raj, *Deepfakes, Copyright, and Personality Rights: A Cross-Jurisdictional Analysis*, 5 J. INFORMATICS EDUC. & RSCH. 1, 12, 41, 57 (2025).
[16] Singh & Panta, supra note 13.
[17] *Id.* at 19.
[18] Chandel & Kundu, supra note 11.

regime that addresses deepfakes as a distinct legal harm while strengthening intermediary accountability, evidentiary safeguards, and digital forensic capacity.[19]

RESEARCH METHODOLOGY

This study adopts a doctrinal legal research methodology and is based exclusively on secondary sources. It examines Article 21 of the Constitution of India and its judicial interpretations, along with key legislations including the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Bharatiya Sakshya Adhiniyam, 2023, the Digital Personal Data Protection Act, 2023, and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules. Government reports, policy documents, judicial decisions and academic literature have also been analysed to evaluate the strengths and limitations of the existing legal framework. Additionally this study undertakes a comparative analysis of legal developments in the United States, the European Union, the United Kingdom, and China to identify approaches relevant to India. Its scope does not include empirical research or technical analysis and is limited to the legal and policy aspects of deepfake impersonation affecting ordinary citizens.

CONSTITUTIONAL PROTECTION OF IDENTITY AGAINST ARTIFICIAL INTELLIGENCE

Following the Supreme Court's decision in Justice K.S. Puttaswamy v. Union of India, informational privacy, personal autonomy, and dignity have acquired greater constitutional significance in discussions concerning digital identity.[20] Building upon this constitutional framework, it is now argued that AI enabled impersonation directly interferes with these constitutional interests by enabling the unauthorised reproduction and manipulation of an individual's likeness without consent, extending beyond physical space to include informational privacy and individual autonomy. The judgment established that personal information forms part of human dignity and that individuals possess a legitimate interest in controlling how such information is collected and used. Although the Court did not address artificial intelligence directly, its reasoning provides an important constitutional basis for examining deepfake impersonation because a person's face, voice, and biometric characteristics are increasingly

[19] Pratishtha Shree, supra note 8 (last visited July 30, 2026).
[20] *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.

treated as forms of personal information. Yet the emergence of Generative Artificial Intelligence exposed an important limitation to these Constitutional rights that traditionally regulated the relationship between the State and the individual. Since, Deepfake impersonation originates from private actors, including private persons or private entities, operating through social media platforms, anonymous online accounts, or commercial AI services, this constitutional framework fails to provide an immediate remedy against private misuse. Victims often have to rely on criminal complaints or intermediary action rather than direct constitutional enforcement. This distinction confirms that constitutional recognition of privacy alone is insufficient to resolve every form of digital impersonation.

The Delhi High Court in Anil Kapoor v. Simply Life India[21] demonstrated the protection of personality rights by reaffirming that an individual's name, voice, image, likeness, and other personality attributes cannot be commercially or otherwise exploited without consent. The judiciary further recognised the limitations of the existing legal framework in TV Today Network Ltd. v. Union of India,[22] a case which challenged the unregulated misuse of artificial intelligence tools, specifically deepfakes and digital impersonation.While declining to issue immediate substantive directions, the court considered the petitioner's contention that the absence of a structured national law leaves ordinary citizens highly vulnerable to exploitation. However, the Court noted that the matter was already under consideration by a committee constituted by the Ministry of Electronics and Information Technology (MeitY) and added that delays in the detection and removal of deepfake content were causing widespread hardship. The court also acknowledged the broader regulatory limitations by thereby reflecting the need for a statutory framework to safeguard the identity and personality rights of ordinary citizens. The decision illustrates the judiciary's recognition of the inadequacy of the present legal remedies against AI enabled misuse of identity. The urgent necessity of this judicial recognition is underscored by alarming real world incidents, such as a recent June 2026 incident in Guwahati, where AI generated explicit images of female students and teachers from a school were created using photographs harvested from social media and circulated without their knowledge or consent. The incident illustrates how deepfake impersonation transcends commercial exploitation, striking directly at the core of an ordinary citizen's fundamental privacy, dignity,

[21] Anil Kapoor v. Simply Life India & Ors., 2023 SCC OnLine Del 6914.
[22] TV Today Network Ltd. v. Union of India, W.P.(C) 6037/2025 (Del. H.C. June 25, 2025).

and personal security. The injury to an ordinary citizen is not the loss of commercial goodwill but the loss of dignity, privacy, and personal security. These constitutional principles establish an important foundation, however constitutional protection alone cannot investigate offences, prosecute offenders, or remove harmful content from digital platforms and these responsibilities fall within the statutory framework.

THE LIMITATIONS OF EXISTING LAWS IN RESPONSE TO DEEPFAKE IMPERSONATION

Since India does not presently regulate deepfake impersonation through a dedicated statute, protection against it is distributed across several laws addressing identity theft, fraud, privacy, defamation, intermediary liability, data protection, and electronic evidence, reflecting a historical development of India's current cyber law framework, as most of the existing legislation was enacted before artificial intelligence acquired the ability to generate convincing synthetic media. Indicating that deepfakes are generally addressed through legal provisions designed for different forms of digital misconduct.[23]

The Information Technology Act, 2000 remains central to this framework as provisions relating to identity theft, cheating by personation, privacy violations, and obscene content allow investigators to prosecute several consequences of deepfake misuse.[24] The Bharatiya Nyaya Sanhita expands this protection through offences involving forgery, defamation, and false electronic records.[25] The Digital Personal Data Protection Act seeks to regulate the collection and processing of personal data, while the Information Technology Rules place responsibilities upon intermediaries to remove unlawful content.[26] When considered individually, each law addresses one aspect of the problem but when considered collectively, they create a layered response that attempts to balance criminal accountability, platform responsibility, and individual rights.

The difficulty lies in the fact that these statutes regulate the consequences of deepfake impersonation more effectively than the technology itself. A victim frequently discovers the synthetic content only after it has been disseminated across multiple platforms. By the time the

[23] Divyanshu Krishna & Abhay Singh, *Regulating Deepfakes: Emerging Forms of Cybercrime and the Adequacy of Indian Cyber Laws*, 2 INT'L J. LEGAL RSCH. & ANALYSIS 194, 198, 200 (2026).
[24] Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
[25] Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023 (India).
[26] Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

offender may be punished through criminal proceedings, reputational damage would have occurred. Similarly, intermediary obligations assist in removing unlawful content, but rapid dissemination means that copied versions frequently remain accessible. The legal framework therefore is predominantly reactive addressing the aftermath of deepfake misuse rather than preventing it.

Data protection law presents another dimension of this challenge as artificial intelligence systems require large volumes of data for training, much of which originates from publicly available photographs, videos, and voice recordings. The Digital Personal Data Protection Act establishes an important framework for consent and lawful processing. However, legal uncertainty remains regarding the secondary use of publicly available biometric information for training generative models. This uncertainty has become increasingly significant as Indian courts have recognised that the development of AI systems depends upon access to extensive datasets, while also acknowledging the need to balance technological innovation with existing legal rights[27]. Consequently, the distinction between lawful collection and lawful reuse of personal data remains unresolved.

Recognising the broader risks posed by AI generated content, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026 introduced a dedicated due diligence framework for synthetically generated content. The amendments require intermediaries to deploy reasonable technical measures to prevent unlawful synthetic content while mandating the clear labelling and, where technically feasible, the embedding of metadata and unique identifiers for permissible AI generated content.[28] Even though these measures reflect a shift towards greater regulatory oversight and platform accountability, their effectiveness ultimately depends upon the ability of investigators, intermediaries, and courts to reliably distinguish authentic digital content from AI generated content.

[27]Arpan Chaturvedi, *Why the Delhi High Court's Order in the OpenAI Case Is a Win for Public Interest*, INDIAN EXPRESS (Dec. 10, 2024), https://indianexpress.com/article/opinion/columns/ai-model-public-interest-delhi-hc-copyright-openai-chatgpt-10807622/ (last visited July 30, 2026).

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

THE EROSION OF TRUST IN ELECTRONIC EVIDENCE

Not long ago, electronic evidence became an essential feature of modern litigation as digital records frequently documented communication, financial transactions, and personal conduct. The law therefore developed on the assumption that while digital files could be manipulated, technical procedures could verify their authenticity before courts relied upon them. Deepfakes complicated this assumption by making synthetic media increasingly difficult to distinguish from genuine content.

The Bharatiya Sakshya Adhiniyam continues the legal framework governing electronic evidence, yet authentication now requires more than confirming the source of a digital file.[29] Courts must increasingly consider whether apparently genuine content has been generated through artificial intelligence. Courts now recognise this growing concern and illustrate an increasing awareness that photographs and videos may require additional corroboration before being accepted as reliable evidence reflecting a broader institutional challenge rather than judicial reluctance to embrace technology. The consequences of these evidentiary challenges extend beyond courtroom procedure, as victims may struggle to prove that AI generated content is false, while accused persons may dismiss authentic evidence by alleging that it is artificially generated. Both situations simultaneously weaken confidence in digital evidence and increase pressure on forensic institutions. Effective enforcement therefore depends upon the ability of investigators and courts to reliably authenticate AI generated content, since statutory protections alone cannot provide effective remedies without credible methods of verification.

COMPARATIVE REGULATORY APPROACHES TO DEEPFAKE IMPERSONATION

The international response has demonstrated that governments increasingly recognise deepfakes as a challenge to democratic institutions, individual rights, and digital trust. While the European Union adopts a preventive, risk based approach by requiring transparency and disclosure of AI generated content, China places greater emphasis on traceability and user verification to identify the origin of synthetic media before it spreads widely.[30] In contrast, the United Kingdom has adopted a more targeted criminal law response by strengthening protection against non

[29] Bharatiya Sakshya Adhiniyam, 2023, No. 47, Acts of Parliament, 2023 (India).
[30] Sree Parvathavarthini S.K. & Santosh Kumar Tiwari, *Deepfake Technology: Legal Challenges and Regulatory Responses*, 6 INDIAN J. LEGAL REV. 774, 784 (2026).

consensual deepfake intimate content, whereas several jurisdictions within the United States have focused on issue specific legislation addressing election related manipulation and digital impersonation.[31] These approaches differ in structure, yet they share a common understanding that regulating artificial intelligence requires more than criminal punishment after harm has occurred. They increasingly combine preventive obligations, platform accountability, technical standards, and user protection. Even though India has begun moving in the same direction through recent regulatory reforms, further integration between constitutional rights, criminal law, data protection, intermediary responsibility, and evidentiary standards remains necessary.

KEY FINDINGS

Absence of Legal Recognition for AI Generated Impersonation

Indian law does not presently recognise deepfake impersonation as an independent legal harm. The analysis demonstrates that deepfake impersonation cannot be adequately addressed through existing legal categories such as identity theft, cheating by personation, defamation, and privacy violations because each addresses only one dimension of AI enabled identity misuse.[32] As a result, the existing legal framework remains fragmented and reactive, regulating the consequences of deepfake impersonation through conventional cyber offences rather than the unauthorised creation of a synthetic identity itself.

Constitutional Protection Requires Effective Statutory Implementation

Article 21 of the Constitution provides the normative foundation for protecting digital identity through the rights to privacy, dignity, and personal autonomy.[33] However, constitutional protection cannot independently safeguard ordinary citizens against deepfake impersonation as such conduct is predominantly committed by private actors using easily accessible Generative AI and digital platforms. While constitutional principles establish the values that the legal system must protect, their practical enforcement depends upon statutory mechanisms capable of preventing, remedying, and deterring deepfake impersonation.

[31] Id.
[32] Information Technology Act, No. 21 of 2000, §§ 66C, 66D, 67, India Code (2000); Bharatiya Nyaya Sanhita, No. 45 of 2023, §§ 319, 336, 356, India Code (2023).
[33] INDIA CONST. art. 21.

Fragmentation of the Existing Statutory Framework

India's statutory framework addresses deepfake related harms through the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Digital Personal Data Protection Act, 2023, and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.[34] However, these laws regulate different aspects of the problem independently and primarily provide legal remedies only after harm has occurred. As a result, ordinary citizens remain reliant on dispersed statutory provisions that collectively address the effects of deepfake impersonation without recognising AI generated impersonation as a distinct legal wrong.

Erosion of Trust in Electronic Evidence

Deepfake technology presents a significant challenge to the authenticity and reliability of electronic evidence. Although the Bharatiya Sakshya Adhiniyam, 2023 modernises the admissibility of electronic records, it was not designed to address the evidentiary risks created by highly realistic AI generated media. As fabricated digital content becomes increasingly difficult to distinguish from authentic recordings, courts and investigative agencies will require greater reliance on digital forensic techniques and expert evidence. This challenge is particularly significant for ordinary citizens, who often lack the technical and financial resources necessary to establish that manipulated digital content is fabricated, thereby increasing their vulnerability within both criminal and civil proceedings.

CONCLUSION

The emergence of Generative Artificial Intelligence has fundamentally challenged the assumption that an individual's digital identity is an authentic representation of that individual. This study demonstrates that while India's existing legal framework provides constitutional and statutory remedies against the harms arising from deepfake impersonation, it remains predominantly fragmented and reactive because it addresses the consequences of AI generated impersonation rather than the unauthorised creation of synthetic identities themselves. The analysis further demonstrates that existing legal protections collectively provide important

[34] Information Technology Act, No. 21 of 2000, India Code (2000); Bharatiya Nyaya Sanhita, No. 45 of 2023, India Code (2023); Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023); Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E), Gazette of India, Extraordinary, pt. II, sec. 3(i) (Feb. 25, 2021), as amended.

safeguards relating to privacy, identity theft, fraud, intermediary responsibility, and electronic evidence. However, these protections were developed independently to address conventional forms of legal injury and therefore are inadequate to respond to the distinctive challenges posed by AI generated impersonation. As a result, ordinary citizens remain dependent upon multiple legal provisions that become effective only after harm has occurred.

Comparative developments examined in this study further indicate that jurisdictions are increasingly adopting preventive regulatory measures by combining platform accountability, transparency obligations, technical safeguards, and targeted statutory protections. Although India has taken important steps through recent regulatory reforms, the existing framework continues to lack a unified legal approach capable of addressing synthetic identity at its source. This study therefore contributes to the growing legal scholarship by arguing that AI generated impersonation should be conceptualised as a distinct legal harm rather than merely another manifestation of existing cyber offences.

In conclusion, the principal challenge is not the absence of legal protection but the absence of legal recognition of AI generated impersonation as a distinct legal harm and meaningful protection for ordinary citizens will require a legal framework that will address AI generated impersonation before irreversible harm occurs while preserving the constitutional values of dignity, privacy, autonomy, and trust in digital identity.