International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

DEEPFAKE TECHNOLOGY AND CRIMINAL LAW REFORM IN INDIA: ADDRESSING SYNTHETIC MEDIA UNDER THE BHARATIYA NYAYA SANHITA, 2023

Niharika Jorwal

Research Scholar
Jaipur National University

Abstract:
Deepfake technology, a rapidly evolving form of artificial intelligence–generated synthetic media, has emerged as a significant threat to individual dignity, democratic integrity, and the administration of criminal justice in India. By enabling the creation of hyper-realistic yet fabricated audio, video, and image content, deepfakes facilitate offences such as identity theft, financial fraud, cyber extortion, electoral misinformation, and non-consensual intimate imagery. The enactment of the Bharatiya Nyaya Sanhita, 2023 (BNS) marks a transformative phase in India's criminal law reform; however, the statute does not expressly define or criminalize the malicious creation and dissemination of synthetic media. This legislative gap raises concerns regarding victim protection, evidentiary admissibility, investigative competence, and proportional punishment. This paper critically examines the applicability of existing BNS provisions relating to forgery, cheating, defamation, and cyber-enabled offences to deepfake-related harms, highlighting doctrinal ambiguities and enforcement challenges. It argues for a structured reform approach that includes a clear statutory definition of synthetic media offences, graded penalties, digital forensic standards, and expedited procedural safeguards for victim redressal. Aligning with Sustainable Development Goals particularly SDG 16 (Peace, Justice and Strong Institutions) and SDG 9 (Industry, Innovation and Infrastructure) the study emphasizes the need for a balanced regulatory framework that fosters technological innovation while safeguarding constitutional rights and public trust. A coherent legislative response under BNS is imperative to ensure accountability, strengthen institutional resilience, and uphold the rule of law in India's digital era.

Keywords: Deepfake Technology, Synthetic Media, Bharatiya Nyaya Sanhita 2023, Criminal Law Reform, SDG 16, Digital Forensics.

1. INTRODUCTION

The rapid advancement of artificial intelligence (AI) has significantly transformed global communication systems, economic structures, and governance frameworks. Among the most disruptive outcomes of AI development is deepfake technology, a form of synthetic media that employs deep learning techniques to generate highly realistic but fabricated audio, video, and visual content (Chesney & Citron, 2019). While deepfake applications may serve legitimate purposes in entertainment, accessibility innovation, and digital creativity, their misuse poses serious threats to criminal justice administration, democratic governance, and constitutional rights. In India, where digital connectivity and social media penetration have expanded dramatically over the past decade, the risks associated with malicious synthetic media are amplified by scale, diversity, and limited institutional preparedness.

The enactment of the Bharatiya Nyaya Sanhita, 2023 (BNS) marks a historic reform in India's criminal law framework, replacing the colonial-era Indian Penal Code, 1860. The BNS seeks to modernize

substantive criminal law to reflect contemporary social and technological realities. However, despite its structural reform, the statute does not explicitly define or criminalize deepfake or synthetic media offences. This legislative silence generates doctrinal ambiguity regarding the applicability of existing provisions relating to forgery, impersonation, defamation, cheating, and cyber-enabled harms. The absence of specific statutory recognition may undermine prosecutorial efficiency, weaken victim protection, and create interpretative inconsistencies in judicial adjudication.

Deepfake misuse has already demonstrated the capacity to disrupt democratic institutions, manipulate electoral discourse, and facilitate technology-enabled gender-based violence. Non-consensual intimate imagery generated through synthetic manipulation disproportionately affects women, thereby implicating constitutional guarantees of equality and dignity under Articles 14, 15, and 21 of the Constitution of India. Addressing such harms aligns with Sustainable Development Goal (SDG) 5, which seeks to eliminate all forms of violence against women and girls, including those facilitated by digital technologies (United Nations, 2015). Similarly, the destabilizing impact of misinformation and fabricated political content directly implicates SDG 16, which emphasizes peace, justice, and strong institutions grounded in the rule of law.

Technological innovation remains essential for national development, economic growth, and digital transformation. SDG 9 encourages innovation and resilient infrastructure, including digital ecosystems. However, innovation without regulatory oversight may produce externalities that threaten social stability and individual rights. Criminal law reform under the BNS must therefore strike a normative balance between promoting technological advancement and preventing its misuse. A forward-looking penal framework should anticipate emerging technological harms rather than react to them retrospectively.

Another dimension of concern involves evidentiary reliability. Digital recordings have traditionally been regarded as persuasive evidence in criminal proceedings. The increasing sophistication of deepfake manipulation undermines confidence in audiovisual authenticity and introduces the phenomenon known as the "liar's dividend," whereby genuine evidence may be dismissed as fabricated (Chesney & Citron, 2019). Such developments risk contaminating judicial fact-finding processes and eroding institutional trust, thereby weakening the broader objectives of criminal justice reform.

India's constitutional jurisprudence recognizes dignity, privacy, and reputation as intrinsic components of the right to life and personal liberty (Justice K.S. Puttaswamy v. Union of India, 2017). Deepfake misuse directly infringes upon these rights, particularly in cases involving fabricated confessions, manipulated speeches, or intimate imagery. Consequently, criminal law reform addressing synthetic media must be anchored in constitutional morality and informed by international human rights standards. Integrating SDG principles into legislative reform provides a normative framework that aligns technological governance with sustainable development, institutional accountability, and inclusive justice.

This study therefore examines the conceptual foundations of deepfake technology and evaluates the adequacy of existing criminal law responses under the Bharatiya Nyaya Sanhita, 2023. By situating the issue within constitutional jurisprudence and Sustainable Development Goals, the analysis argues for targeted reform to address synthetic media harms while preserving innovation and democratic resilience.

2. CONCEPTUAL AND TECHNOLOGICAL FRAMEWORK OF DEEPFAKE TECHNOLOGY

Deepfake technology derives from "deep learning," a subset of machine learning that utilizes artificial neural networks to identify patterns within extensive datasets. A commonly employed mechanism is the Generative Adversarial Network (GAN), in which two neural networks the generator and the discriminator operate in competition. The generator produces synthetic outputs, while the discriminator evaluates

authenticity; through iterative refinement, the system produces increasingly realistic fabricated media (Goodfellow et al., 2014).

Technologically, deepfakes involve techniques such as facial mapping, face-swapping, voice cloning, and lip-synchronization. Facial mapping overlays one individual's facial features onto another's image or video. Voice cloning replicates speech patterns and tonal characteristics based on limited audio samples. With the proliferation of open-source software and commercially accessible AI tools, the technological barrier to producing synthetic media has significantly declined. Consequently, malicious actors no longer require advanced technical expertise to generate deceptive content.

The dual-use character of deepfake technology complicates regulatory responses. Legitimate applications include cinematic visual effects, digital heritage reconstruction, accessibility tools for individuals with speech impairments, and educational simulations. These uses align with SDG 9, which promotes innovation and sustainable industrial development. However, the same technology can be weaponized for criminal purposes, including impersonation scams, financial fraud, political misinformation, and non-consensual sexual content (Paris & Donovan, 2019).

Financial crimes facilitated by deepfakes have emerged globally, with AI-generated voice simulations used to authorize fraudulent corporate transactions. Such conduct intersects with traditional offences of cheating and fraud but demonstrates enhanced sophistication due to technological manipulation. Similarly, reputational harms arise when fabricated videos depict individuals engaging in unlawful or immoral conduct. In electoral contexts, manipulated speeches or inflammatory statements attributed to political leaders may incite unrest or distort democratic processes, thereby undermining SDG 16's objective of strengthening institutions and promoting peaceful societies.

A particularly alarming dimension involves gender-based digital abuse. Non-consensual synthetic intimate imagery disproportionately targets women and marginalized individuals, reinforcing structural inequalities in digital spaces. The gendered nature of such harm underscores the relevance of SDG 5 and SDG 10, which emphasize equality and reduced inequalities. Criminal law reform must therefore address both technological misconduct and its discriminatory impact.

Evidentiary implications present an additional challenge. Courts traditionally rely upon audiovisual evidence to corroborate testimony and establish factual narratives. The increasing realism of deepfakes erodes confidence in such evidence and complicates authentication processes. Forensic detection tools exist but remain engaged in a technological arms race with generative models. Without standardized forensic protocols and institutional capacity-building, investigative agencies may struggle to identify manipulated content accurately.

Jurisdictional complexity further complicates enforcement. Deepfake content may be generated in one country, hosted on servers in another, and disseminated globally within seconds. This transnational character necessitates international cooperation and harmonization of cybercrime frameworks. Domestic criminal law reform must therefore incorporate mechanisms that enable cross-border investigation and digital evidence preservation.

From a doctrinal perspective, existing penal provisions under the Bharatiya Nyaya Sanhita, 2023 relating to forgery, impersonation, and cheating may partially encompass deepfake-related misconduct. However, these provisions were not drafted with AI-generated synthetic media in contemplation. The absence of a clear statutory definition of synthetic media offences risks inconsistent judicial interpretation and

inadequate deterrence. A principled reform approach would include explicit recognition of malicious synthetic media creation, graded penalties based on harm, and enhanced procedural safeguards.

Deepfake technology embodies both the promise and peril of AI-driven innovation. While contributing to digital advancement and economic growth, it simultaneously generates novel criminal risks that challenge traditional legal doctrines. A sustainable regulatory framework under the Bharatiya Nyaya Sanhita, 2023 must integrate technological literacy, constitutional safeguards, and SDG-aligned governance principles to ensure that innovation proceeds without compromising justice, equality, and institutional integrity.

3. DOCTRINAL ANALYSIS OF THE BHARATIYA NYAYA SANHITA, 2023 IN ADDRESSING DEEPFAKE-RELATED OFFENCES

The Bharatiya Nyaya Sanhita, 2023 (BNS) represents a structural reform of India's substantive criminal law. While the statute modernizes language and reorganizes offences to reflect contemporary realities, it does not expressly recognize synthetic media or deepfake technology as a distinct category of criminal wrongdoing. This doctrinal silence raises important interpretative challenges concerning the applicability of existing penal provisions to AI-generated manipulation.

Deepfake-related misconduct may potentially fall within traditional categories such as forgery, cheating, impersonation, defamation, obscenity, and identity theft. The offence of forgery under criminal law historically involves the making of a false document or electronic record with intent to cause damage or injury. In the context of deepfakes, a manipulated video or AI-generated audio recording may qualify as a "false electronic record." However, the statutory language was originally conceptualized in an era where falsification typically involved tangible alteration or fabrication of documents. Deepfake technology, by contrast, produces entirely synthetic representations that may not neatly align with the conventional understanding of document-based forgery.

Similarly, provisions relating to cheating and personation could theoretically apply where deepfakes are used to impersonate individuals for financial gain. Voice-cloning scams and AI-generated executive impersonation schemes demonstrate how synthetic media enhances fraudulent capability. Yet, doctrinal reliance on general cheating provisions may be insufficient in capturing the aggravated harm caused by technologically sophisticated deception. The enhanced scale, speed, and anonymity facilitated by AI tools necessitate a calibrated penal response with proportionate sentencing frameworks.

Defamation provisions may also extend to deepfake-generated reputational harm. Fabricated videos depicting individuals engaging in criminal or immoral acts may satisfy the elements of publication and injury to reputation. However, deepfakes amplify harm through virality and permanence in digital spaces. Once disseminated, synthetic content may be replicated across platforms beyond effective removal. This digital irreversibility intensifies the injury to dignity and privacy, which are constitutionally protected under Article 21 (Justice K.S. Puttaswamy v. Union of India, 2017). The BNS does not currently differentiate between conventional defamatory statements and AI-manufactured audiovisual fabrications that carry heightened evidentiary credibility.

A particularly pressing concern involves gender-based harm through non-consensual intimate imagery generated using deepfake technology. Although obscenity-related provisions may be invoked, the absence of explicit statutory recognition of synthetic sexual exploitation limits victim-centric remedies. Such conduct directly undermines SDG 5, which calls for the elimination of violence against women in public and private spheres (United Nations, 2015). Criminal law reform must therefore adopt a gender-sensitive lens, recognizing the disproportionate impact of deepfake abuse on women and marginalized communities.

Beyond substantive offences, procedural challenges emerge in evidentiary authentication. The increasing realism of synthetic media complicates the admissibility and evaluation of digital evidence. Courts must rely on forensic analysis to determine authenticity, yet India's cyber forensic infrastructure remains unevenly distributed. Without standardized forensic protocols and trained personnel, the risk of evidentiary misinterpretation increases. This threatens the broader objectives of SDG 16, which emphasizes effective, accountable, and transparent institutions.

Furthermore, the phenomenon known as the "liar's dividend" permits accused individuals to dismiss genuine audiovisual evidence as fabricated (Chesney & Citron, 2019). This defensive strategy undermines prosecutorial credibility and complicates fact-finding. The BNS does not currently incorporate procedural safeguards or evidentiary presumptions tailored to synthetic media contexts. A comprehensive reform approach would include statutory definitions of malicious synthetic media, graded penalties based on severity of harm, mandatory forensic authentication standards, and victim compensation mechanisms.

The transnational nature of deepfake dissemination further complicates enforcement. Synthetic content may originate outside India while causing harm within its jurisdiction. Effective prosecution therefore requires harmonization with cybercrime cooperation frameworks and cross-border evidence preservation mechanisms. Absent explicit statutory recognition, investigative agencies may encounter jurisdictional ambiguity and procedural delays.

While existing provisions of the Bharatiya Nyaya Sanhita, 2023 may partially encompass deepfake-related misconduct, they do so indirectly and inconsistently. A forward-looking criminal justice framework must explicitly define and criminalize malicious synthetic media creation and dissemination. Such reform would strengthen institutional resilience, uphold constitutional dignity, and align with SDG 16's commitment to rule-of-law governance.

4. COMPARATIVE JURISDICTIONAL APPROACHES AND THE NEED FOR REFORM IN INDIA

Comparative analysis reveals that several jurisdictions have begun addressing deepfake harms through targeted legislation. In the United States, certain states such as California and Texas have enacted laws criminalizing deepfake political misinformation and non-consensual intimate deepfakes. These statutes recognize the unique societal harm posed by synthetic media, particularly during electoral processes. By focusing on electoral integrity, such reforms align with democratic governance principles analogous to SDG 16.

At the federal level, while the United States lacks a comprehensive deepfake statute, legislative proposals have sought to regulate malicious synthetic media. The emphasis has been on balancing First Amendment protections with safeguards against fraud and harassment. This balancing exercise reflects a broader global challenge: reconciling freedom of expression with the need to prevent technologically facilitated harm.
The European Union has adopted a more structured regulatory approach through its Artificial Intelligence regulatory framework. The EU AI regulatory model classifies AI systems based on risk categories, imposing stricter obligations on high-risk systems. Deepfake content, particularly where capable of causing public harm, is subject to transparency obligations requiring clear labeling and disclosure. This preventive regulatory model emphasizes accountability and transparency, reinforcing institutional trust and aligning with SDG 9's objective of responsible innovation.

China has introduced regulations requiring explicit labeling of synthetic content and imposing liability on service providers that fail to prevent misuse. These regulatory strategies prioritize state oversight and

content traceability. Although differing in normative orientation, such approaches demonstrate recognition of synthetic media as a distinct legal concern requiring specific regulation.

In contrast, India's current framework primarily relies on general criminal provisions under the Bharatiya Nyaya Sanhita, 2023 and supplementary digital regulations. The absence of explicit deepfake legislation places India in a reactive posture. Given India's vast digital user base and socio-political diversity, failure to proactively regulate synthetic media may expose democratic processes, financial systems, and vulnerable communities to substantial harm.

Comparative experience suggests that effective regulation requires a multi-layered approach: (1) clear statutory definitions of synthetic media manipulation, (2) graded criminal liability based on intent and harm, (3) mandatory disclosure requirements for AI-generated content, (4) institutional investment in digital forensic infrastructure, and (5) international cooperation mechanisms. Integrating such measures within the Bharatiya Nyaya Sanhita, 2023 would modernize India's penal framework while preserving constitutional safeguards.

The reform imperative also intersects with SDG 17, which emphasizes global partnerships for sustainable development. Cross-border cybercrime enforcement depends upon mutual legal assistance treaties, digital evidence-sharing protocols, and collaborative forensic research. Deepfake regulation cannot be confined within domestic boundaries due to its inherently transnational character.

Moreover, regulatory design must incorporate proportionality and due process. Overbroad criminalization risks chilling legitimate artistic expression and technological research. Therefore, legislative drafting should differentiate between malicious intent and legitimate use, ensuring that criminal liability attaches only where demonstrable harm or fraudulent intent exists. Such calibrated reform would reflect constitutional commitments to free expression while safeguarding dignity and security.

Comparative jurisdictions demonstrate increasing recognition of deepfake harms as distinct legal challenges. India's criminal law reform under the Bharatiya Nyaya Sanhita, 2023 provides a historic opportunity to integrate explicit synthetic media provisions into the penal code. Aligning such reform with Sustainable Development Goals particularly SDG 5, SDG 9, SDG 16, and SDG 17 would ensure that technological governance contributes to inclusive justice, institutional integrity, and sustainable democratic development.

5. REFORM PROPOSALS: TOWARDS A COMPREHENSIVE LEGAL FRAMEWORK FOR DEEPFAKE REGULATION IN INDIA

The proliferation of deepfake technology necessitates a structured and forward-looking reform of India's criminal law framework under the Bharatiya Nyaya Sanhita, 2023 (BNS). Although the BNS modernizes the structure and language of substantive criminal law, its failure to explicitly recognize synthetic media manipulation creates a significant normative and operational gap. A coherent reform strategy must begin with statutory recognition of malicious synthetic media as a distinct category of criminal wrongdoing. The absence of definitional clarity leads to interpretative inconsistency when courts attempt to fit deepfake-related harms within traditional offences such as forgery, cheating, defamation, or impersonation. While these provisions may partially apply, their indirect application does not sufficiently address the technological sophistication, scale, and virality of AI-generated manipulation. Therefore, legislative reform should incorporate a clear statutory definition encompassing the intentional creation or dissemination of AI-generated or AI-altered audiovisual content with knowledge of falsity and intent to cause harm, secure unlawful gain, or mislead the public. Such clarity would enhance prosecutorial efficiency, strengthen deterrence, and align with the rule-of-law objectives embedded in Sustainable

Development Goal (SDG) 16, which emphasizes effective and accountable institutions (United Nations, 2015).

Reform must also adopt a proportional and graded liability framework that differentiates between varying degrees of harm. Not all synthetic media creation warrants criminal sanction; legitimate artistic, educational, or research uses must remain protected. However, aggravated circumstances such as electoral interference, financial fraud, communal incitement, or non-consensual intimate imagery should attract enhanced penalties reflecting the gravity of harm. A calibrated structure ensures that criminalization remains consistent with constitutional guarantees of free expression while addressing malicious conduct. In this regard, the principle of proportionality remains central to balancing innovation and accountability. A particularly urgent dimension of reform concerns gender-based digital abuse. Empirical evidence demonstrates that non-consensual deepfake pornography disproportionately targets women, reinforcing structural inequalities in digital environments (Chesney & Citron, 2019). The psychological trauma, reputational damage, and social stigma associated with such abuse extend far beyond traditional notions of obscenity. Criminal law must therefore explicitly criminalize synthetic sexual exploitation irrespective of whether the depicted act occurred in reality. Such reform directly advances SDG 5, which seeks to eliminate all forms of violence against women and girls, including technology-facilitated abuse. Victim-centric safeguards, including confidentiality protections, expedited takedown orders, and access to compensation mechanisms, are essential to prevent secondary victimization. The constitutional recognition of privacy and dignity as intrinsic to Article 21 (Justice K.S. Puttaswamy v. Union of India, 2017) further underscores the imperative of incorporating gender-sensitive provisions within the BNS framework.

Another critical reform area involves evidentiary standards and forensic capacity-building. Deepfake technology undermines the reliability of audiovisual evidence, which has traditionally served as persuasive proof in criminal trials. The phenomenon known as the “liar’s dividend” permits accused individuals to dismiss authentic recordings as fabricated, thereby complicating judicial fact-finding (Chesney & Citron, 2019). Legislative reform should therefore incorporate procedural safeguards requiring forensic authentication in cases where the authenticity of digital content is disputed. Establishing standardized protocols for digital evidence examination, accreditation of forensic experts, and mandatory preservation orders would reduce evidentiary uncertainty. Investment in AI-based detection tools and specialized cyber forensic laboratories is equally necessary to ensure institutional preparedness. Such measures contribute directly to SDG 16’s emphasis on strengthening institutional integrity and transparency.

In addition to substantive criminalization and procedural safeguards, reform must address the role of digital intermediaries. Given the rapid dissemination of synthetic media across online platforms, preventive regulation should incorporate transparency and accountability obligations for intermediaries. Requiring platforms to implement reporting mechanisms, cooperate with law enforcement investigations, and comply promptly with judicial takedown directives can mitigate harm without imposing disproportionate censorship. Comparative regulatory models emphasize transparency obligations such as labeling AI-generated content as a preventive strategy. Such measures align with SDG 9, which promotes responsible innovation and resilient digital infrastructure. However, regulatory design must remain carefully balanced to avoid chilling legitimate speech or technological research. Liability frameworks should focus on willful negligence or failure to comply with lawful directives rather than imposing blanket censorship obligations.

The threat posed by deepfakes to electoral integrity further justifies targeted reform. Fabricated political speeches, manipulated campaign messages, and communal incitement through synthetic videos may distort democratic discourse and undermine public trust in electoral processes. Aggravated penalties for

deepfake misuse during election periods would signal the seriousness of such conduct and reinforce democratic stability. Electoral authorities may also be empowered to coordinate with cybercrime units to implement rapid verification and public clarification mechanisms. Safeguarding electoral integrity reflects the normative commitments embedded in SDG 16, which emphasizes peaceful and inclusive societies governed by accountable institutions.

Finally, the transnational nature of deepfake dissemination necessitates enhanced international cooperation. Synthetic media may be generated in one jurisdiction, hosted in another, and viewed globally within seconds. Domestic criminal law reform must therefore be complemented by strengthened mutual legal assistance mechanisms and cross-border evidence-sharing protocols. International collaboration in AI detection research and forensic innovation would enhance enforcement capacity while promoting harmonized regulatory standards. Such cooperation aligns with SDG 17, which underscores the importance of global partnerships in addressing complex transnational challenges. Without coordinated enforcement, domestic legislation may prove insufficient in addressing cross-border digital harms.

Collectively, these reform proposals envision a holistic framework that integrates substantive criminalization, procedural modernization, institutional strengthening, platform accountability, electoral safeguards, and international collaboration. The Bharatiya Nyaya Sanhita, 2023 provides an institutional foundation for such reform, but its effectiveness depends upon proactive adaptation to emerging technological realities.

6. CONCLUSION

Deepfake technology represents one of the most consequential challenges confronting contemporary criminal law systems. As artificial intelligence continues to evolve, the capacity to fabricate hyper-realistic audiovisual content threatens individual dignity, democratic governance, financial security, and evidentiary integrity. India's transition from the colonial-era penal code to the Bharatiya Nyaya Sanhita, 2023 marks a transformative moment in criminal law reform. Yet, the absence of explicit statutory recognition of synthetic media offences reveals a critical gap that must be addressed through principled legislative intervention.

Existing offences relating to forgery, cheating, impersonation, and defamation offer partial remedies but fail to capture the distinct nature of AI-generated manipulation. Deepfakes differ from conventional falsification due to their technological sophistication, virality, and capacity to erode epistemic trust in audiovisual evidence. The resulting uncertainty undermines prosecutorial effectiveness and risks weakening public confidence in judicial institutions. Without targeted reform, the criminal justice system may struggle to respond adequately to technologically mediated harm.

Integrating Sustainable Development Goals into the reform discourse provides a normative framework for balancing innovation with accountability. SDG 5 emphasizes the elimination of gender-based violence, underscoring the urgency of addressing non-consensual synthetic sexual exploitation. SDG 9 promotes innovation but demands responsible technological governance. SDG 16 calls for strong institutions, rule-of-law adherence, and transparent justice systems capable of adapting to emerging challenges. SDG 17 highlights the necessity of international cooperation in confronting transnational digital threats. These goals collectively reinforce the need for a comprehensive and forward-looking regulatory approach.

Reform under the Bharatiya Nyaya Sanhita, 2023 must therefore move beyond reactive application of traditional offences and embrace explicit recognition of malicious synthetic media. Incorporating graded liability structures, evidentiary safeguards, gender-sensitive protections, platform accountability, and cross-border enforcement mechanisms would modernize India's penal framework in accordance with

constitutional principles. The recognition of privacy and dignity as fundamental rights (Justice K.S. Puttaswamy v. Union of India, 2017) further mandates legislative responsiveness to technologically facilitated violations.

Ultimately, deepfake regulation is not solely a matter of criminalization but of safeguarding democratic resilience and institutional credibility. In an era where digital authenticity can no longer be presumed, the legitimacy of the criminal justice system depends upon its capacity to adapt. Proactive, SDG-aligned reform under the Bharatiya Nyaya Sanhita, 2023 would ensure that technological advancement proceeds in harmony with justice, equality, and sustainable development. By embracing anticipatory governance rather than reactive enforcement, India can position itself at the forefront of responsible AI regulation while preserving constitutional values and public trust.

REFERENCES:

1. Chesney, R., & Citron, D. K. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review, 107*(6), 1753–1820.
2. Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., & Bengio, Y. (2014). Generative adversarial nets. *Advances in Neural Information Processing Systems, 27*, 2672–2680.
3. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
4. Paris, B., & Donovan, J. (2019). Deepfakes and cheap fakes: The manipulation of audio and visual evidence. *Data & Society Research Institute*.
5. United Nations. (2015). *Transforming our world: The 2030 agenda for sustainable development*. United Nations.
6. Chesney, R., & Citron, D. K. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review, 107*(6), 1753–1820.
7. European Parliament & Council of the European Union. (2024). *Artificial Intelligence Act*. Official Journal of the European Union.
8. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
9. Paris, B., & Donovan, J. (2019). Deepfakes and cheap fakes: The manipulation of audio and visual evidence. *Data & Society Research Institute*.
10. United Nations. (2015). *Transforming our world: The 2030 agenda for sustainable development*. United Nations.
11. Chesney, R., & Citron, D. K. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review, 107*(6), 1753–1820.
12. European Parliament & Council of the European Union. (2024). *Artificial Intelligence Act*. Official Journal of the European Union.
13. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
14. United Nations. (2015). *Transforming our world: The 2030 agenda for sustainable development*. United Nations.