

Regulating Deepfake-Related Crimes in India: A Critical Analysis of the Information Technology Act and Bharatiya Nyaya Sanhita, 2023

¹Dr. Purnima Singh*, ²Lotus Khanna, ³Ankur Tharwan, ⁴Mohd Zishan Khan and ⁵Dr. Pawan Kumar

¹Assistant Professor, Department of Political Science, College of Commerce Arts and Science, Patliputra University, Patna, Bihar-800020

purnima.politicalscience@gmail.com/ ORCID Id: 0009-0005-7285-6208

²Student, Christ Deemed to be University, Delhi NCR

khannalotus24@gmail.com/ ORCID Id: 0009-0002-3359-6288

³Founder, EMS Academy, 82/121 Sector 8 Pratap Nagar Sanaganer Jaipur, Rajasthan-302033

ankuremsacademy@gmail.com/ ORCID id: 0009-0009-4006-5267

⁴Assistant Professor, School of Legal Studies, CGC University, Mohali, 140307, Punjab, India

mohdzishan.j4114@cgcuniversity.in/ ORCID Id - 0009-0000-4626-9345

⁵Assistant Professor, College of Law & Legal Studies, Teerthankar Mahaveer University, Moradabad

pawankumar.law@tmu.ac.in/ ORCID - 0009-0003-1983-0370

*Corresponding Mail: purnima.politicalscience@gmail.com

Abstract:

The study explores the contextual problems with the already available responses and explores the applicability of the various statutory regulations that govern impersonation, forgery and fraud, obscenity and defamation and the admissibility and proof of electronic information. Through careful study of the court interpretation, regulatory rhetoric and legislative language, the study demonstrates structural shortcomings, normative ambiguity, and symptoms of evidentiary failure that have impeded successful prosecution. The study finds that the current India's legal framework has major gaps. The provisions of the Information Technology Act 2000, Indian Penal Code 1860, The Bharatiya Nyaya Sanhita, 2023 (BNS) and upcoming data protection laws offer limited protection with limited clarifications on the issues deepfakes pose. The study highlights the growing concern over the threat issues of authenticity and rigidities of deepfake technologies; it thoroughly examines the legal provisions made by the Information Technology Act, 2000 and Bharatiya Nyaya Sanhita, 2023, and contemplates the evidentiary provisions mentioned in the Bharatiya Sakshya Adhiniyam, 2023. The results suggest that the existing legislation covers individual cyber offences, yet there isn't a general and specialised statute laying out the production, dissemination and application of deepfakes in India. The report also highlights issues related to the verification of synthetic content, liability issues, enforcement and the need for specific legislative and tech solutions to tackle deepfake related abuses efficiently. The study calls for a three-pronged approach to the legal solution which very specifically addresses the problem. Right at the end, it also stresses the need to improve the India's legal framework, which is a need not a futuristic plan and gives pause to confidence towards the Digital Economy.

Keywords: Deepfake Technology, Artificial Intelligence, Cybercrime, Information Technology Act, Bharatiya

Nyaya Sanhita 2023, Digital Evidence, Identity Theft, Privacy Rights, Misinformation, Platform Accountability, Cyber Law, India.

1. INTRODUCTION

Deepfake technology, as it is known, is an advanced form of Artificial Intelligence (AI) which creates realistic, but fake, AV content on the basis of replacing one person with another. The term is a blend of “deep learning” and “fake,” referring to the architecture of the neural network used to create this synthetic media. There are different sets of technology each with its particular legal and social issues. For some reason, the technological advances of the twenty first century have provided means of communication that not only improve human communication, but at the same time have made them means of distortion by which they can be distorted beyond all recognition. Of these, the one that has unsettled the most is ‘deepfake’ – a term that is derived from ‘deep learning’ and ‘fake’ that means hyper-realistic synthetic audio-visual content generated by artificial neural networks¹.

The first step in establishing the regulatory framework for deepfakes is to understand how they work, but not in computer science or by programming them, but rather in sufficient detail to understand why they present new issues for regulation that are not applicable to previous forms of digital manipulation. Deepfake technology works on a whole other principle. It uses deep neural networks—the networks are models that are loosely based on the way a living being’s brain works—which are trained using lots of data from a person’s photographs, videos and voice recordings².

In this study, the author argues that India should be wary of addressing deepfakes as just moral issues or a nuisance, as these are human rights abuses as well. Doctrinally, by including prevention measures for synthetic exploitation elements in the understanding of “Article 21” jurisprudence and international obligations, the law could be a reflection of the real experiences of victims in the current digital age. Deepfakes technology first came to light in 2020, and caused concerns about the social impacts. The biggest concern with deepfakes is that they merge the lines between true and false, making it harder for people to tell which is which when they are consuming media. The most troubling aspect of a deepfake is its ability to obscure that distinction between reality and fabrication, and thus making it more problematic to distinguish among genuine and altered media when people are consuming them. Not only does this put individual reputations but also public trust in media outlets at risk images³. Over the last 10 years, deepfake technology has rapidly evolved to make pricier and more sophisticated deepfakes available. Currently, it predominantly presents itself in three principal forms, each susceptible to considerable abuse and capable of inciting issues:

- Face swapping: It is a technique that entails substituting one person’s face with that of another in video or picture media. It is widely used to make an appearance or witness to an event appear to have occurred or to have been witnessed when it did not or was not.
- Lip syncing: This is changing the video so that an individual appears to be saying words that weren’t said by them. This technique is typically used in AV misinformation, especially in political or libellous situations.

¹ Kashyap, S. (2025). The Digital Mirage: India’s Evolving Legal Battle Against Deepfake Technology. *SCRIPTed: A Journal of Law, Technology & Society*, 22(2), 162-226.

² ADABALA, D. S. (2026). When Technology Lies: Deepfake and Criminal Law in India. Available at SSRN 6665081

³ YADAV, J., & Parihar, A. (2025). Deepfakes: The Nexus of Technology and Crime. Available at SSRN 5296147.

- Puppetry (Puppet Technique): The puppet technique evokes deceptive movements and/or gestures by artificially enlivening the likeness of an individual. This often leads to having extracorporeal or extramudial movements attributed to real people and makes identification and decoding difficult⁴.

Deepfakes are therefore classified higgledy pickled with the real photos. Current charges can be expanded to include information created by another source, but this concerns not autonomy but morality and public order. By applying general concepts of fraud, instead of specifically acknowledging personal infringement of copyright laws, in cases where deepfakes are used in fraudulent activities, such as investment characteristics fraud, victims will lose the ability to have a doctrinal remedy for their harm and, consequently, those of significant value will be reduced to status offence cases⁵.

A multitude of well-known deepfakes proliferate online and are accessible on prominent platforms like YouTube. The inaugural and arguably most renowned deepfake is the “2018 video of Barack Obama”, in which he sarcastically cautions against the perils of deepfakes, a warning he never actually delivered. Other deepfakes include celebrity pornographic films and the distortion of politicians' images, such as “substituting Angela Merkel's visage with that of Donald Trump or vice versa with Mr. Bean”. Deepfakes possess the potential to not only superimpose images in a video but also to create original material. This signifies authentic photographs of human faces, produced as a consequence of AI analysing other human images⁶.

Regrettably, one of the limited empirical study on deepfakes offers preliminary evidence that concerningly supports this philosophical perspective. In a study examining the impact of deepfakes on confidence in news, Vaccari and Chadwick discovered that while individuals were unlikely to be entirely deceived by a deepfake (at least given the technology employed), exposure to the deepfake heightened their overall doubt regarding media. When dire expectations were confirmed, participants' belief in news diminished, which is in line with Fallis's theory of epistemic threats⁷.

Several countries around the world have started addressing gender-based crimes related to AI. So, the UK's Online Safety Act 2023, and a recent amendment to South Korea's Sexual Violence Crime Act, ban the production and dissemination of sexual deepfakes. India currently does not have any measure specifically dedicated to deepfakes and this paucity of legislation reflects an urgent need to reinvision the interplay between technological damages and gender equality in the digital era. This study seeks to critically examine the increasing risks of AI-facilitated crimes against women in India in relation to the new phenomena 'deepscams' and online harassment, analyse and highlight gaps in the current legal regime and make comparative and reformative suggestions based on international standards and instruments⁸.

- Though most countries agree on the importance of deep fake regulation, some countries have already implemented certain laws to address this problem, like the UK, South Korea, and China, India is still facing a lack of a broader legislative approach to tackling it. Consent & data security

4 Ramluckan, T. (2024). Deepfakes: The legal implications. *International Conference on Cyber Warfare and Security*, 19(1), 282–288. <https://doi.org/10.34190/iccws.19.1.2099>.

5 Thakur, D. S. (2025). Deepfakes as Human Rights Violations: Rethinking Dignity and Privacy in India. *Available at SSRN 5532383*.

6 Karnouskos, S. (2020). Artificial intelligence in digital media: The era of deepfakes. *IEEE transactions on technology and society*, 1(3), 138-147.

7 Hancock, J. T., & Bailenson, J. N. (2021). The social impact of deepfakes. *Cyberpsychology, behavior, and social networking*, 24(3), 149-152.

8 S. Yumkhaibam, Digital Gender-Based Violence: Power, Inequality, and the Struggle for Online Safety in India, Academia.edu (2025), available at: https://www.academia.edu/download/124247485/Power_Inequality_and_Struggle_for_Online_Safety_Su_shmita_.pdf.

provisions in the “Personal Data Protection Bill, 2023” and “Digital India Act” proposals remain - but do not explicitly criminalise impersonation (AI) and synthetic pornography. This lack of rule making results in:

- Extended FIR's as it's been noticed that the police do not consider the deepfakes as criminal activity.
- No Precedents to guide courts on accepting evidence provided by AI.
- Victim-blaming (the burden of proof usually falls on the woman to prove the content is wrong)⁹.

Deep fake content can be created for a variety of purposes, including entertainment, but can also be used for purposes such as retribution, extortion, and identity theft as well as for many other purposes. As a result, deepfakes have had a significant impact on the landscape of deception, from trivial topics like celebrity gossip to influencing opinion, making choices and ruining reputations. With the rise of AI-generated content becoming more challenging to discern fact from fiction, it becomes even more difficult to distinguish fact from fiction. The biggest of these deepfake technology examples is face-swapping technology. Generates realistic but completely made up film through a method using generative adversarial networks (GANs) to easily replace facial features from video sources. Similarly, voice synthesis and voice cloning technologies have become equally worrisome, as in the recent example of the Bombay High Court case, *Asha Bhosle vs Mayk Inc.*, where the rapidly growing technology of voice cloning was used to create resultants which imitated the playback singer's distinct voice and backup music style¹⁰.

2. LITERATURE REVIEW

The existing literature in the field of deep fake crimes and Indian laws in relation to it are summarised. The scholar has surveyed, critically, the academic literature, legal commentaries, policy research, and judicial discussions about the challenges raised by deepfakes. Previous scholarly work has mainly centred on the rise of deepfakes as a form of cybercrime. Saggu, R., et al., (2025)¹¹ highlighted the proliferation of deepfakes as a menace brought by advancements in artificial intelligence and machine learning in creating and disseminating online content. With the support of a technique like generative adversarial networks (GANs), highly realistic but totally fictional media can be created.

Beyond its current applications, the potential of this technology is seen in its use for more enhanced accessibility in film production, online education, and for persons with an impair. In the theatre of application, this technology can be used in several sectors including film production, online education and bolstering accessibility for those with impairments. Omotoso, O. (2025)¹² discuss the current shortcomings in detection methods and the urgent need for robust deepfake countermeasures in 2025, highlighting the need for substantial legal reform to counteract deepfake misuse and the adoption of advanced content verification systems. Public awareness and education play a key role in mitigating vulnerabilities and building preparedness to withstand threat from deepfake technology. It seeks to suggest ways for reconciling innovation with responsibility in a dynamic digital environment.

⁹ Sharma, R. (2025). Artificial Intelligence and Gender-Based Crimes in India with Reference to Deepfakes and Online Harassment. *Supremo Amicus*, 38, xxiv.

¹⁰ Kashyap, S. (2025). The Digital Mirage: India's Evolving Legal Battle Against Deepfake Technology. *SCRIPTed: A Journal of Law, Technology & Society*, 22(2), 162-226.

¹¹ Saggu, R., & Kumar, A. (2025). Digital Replicas and Financial Crimes. *Traditional and Contemporary Criminal Jurisprudence (University Book House Pvt Ltd, Jaipur 2025 forthcoming)*.

¹² Omotoso, O. (2025). Synthetic Media in Modern Banking: Accountability, Governance and Consumer Protection in the Age of Digital Fraud. *Governance and Consumer Protection in the Age of Digital Fraud (October 10, 2025)*.

Hickerson, A., et al., (2025)¹³ have paid attention to the fact that deep fake technology is rapidly growing and can be harmful to personal privacy, financial security, and social peace in India. This article suggests that the current Indian legal regime, namely the Information Technology Act of 2000, is not robust enough to govern the new set of offences and Information Technology and not be technologically savvy. However, current laws fail to account for the different types and severities of harm that are being inflicted by hyper-realistic forms of synthetic media, leaving those who have suffered harm without recourse.

Kashyap, S. (2025)¹⁴ significant contributions include the first comprehensive legal analysis of the complex emerging legal landscape around deepfakes in India, evidence-informed policy recommendations and a smart plan to act that considers urgent policy enforcement needs and future institutional changes. In the ever increasingly digital world, the study positions India to be at the front seat in leading the global governance in the era of synthetic media and protect citizens against AI-generated frauds. In this phase Seth, N., Patel, N., et al., (2024)¹⁵ examine real-life case studies from newspapers and articles which show authenticity and complaints of the complainant. This doctrinal study will try to answer the following questions; whether the use of deepfake images violates the right to privacy and whether the right to privacy is a constitutional right for the people. It's also to look into the issue of how one can be manipulated by an unknown person. Legislative framework is analyzed and existing and necessary laws and regulations to respond to deepfakes are identified.

Guruswamy, M. (2017)¹⁶ reviews the legal issues arising out of deepfakes and AI- induced misinformation in India, highlighting the adequacy of existing laws and amendments to the intermediary laws in India. The report evaluates judicial answers, regulatory promises and achievements, and looks at the gaps and suggests amendments to address the evolving threats posed by AI. It argues that India, while having taken some steps to regulate synthetic media, needs robust and flexible regulatory frameworks due to the absence of an appropriate legislation and enforcement challenges. Birrer, A., et al., (2025)¹⁷ underscores the advent of deepfakes has generated apprehensions among scholars, policymakers, and the general populace. However, a lot of problems stem from uneasiness instead of any evidence. This article summarizes the current situation and state of the art on deepfakes based on the results of a thorough empirical research review. It also examines and critically examines the approach given by the regulations worldwide using the qualitative content analysis of the policy and legal texts.

Buo, S. A. (2020)¹⁸ proclaimed that the deepfake technology has reached a new level of complexity. Sexting, audio and video recordings, photos and video calls can now be edited and used to trick and deceive people and businesses. This indicates an increasing risk to international institutions and to people that needs to be addressed. The current research offers an overview of deepfakes, benefits for society, and how the deepfake technology works. Highlights the risks of deepfakes to enterprises, political institutions and judiciaries around the world. The study will also explore some of the solutions to deepfakes and conclude with recommendations for additional research.

¹³ Hickerson, A., Schwartz, C., & Wright, M. (2025). *Fake-Checking: A Journalist's Guide to Deepfakes*. Taylor & Francis.

¹⁴ Kashyap, S. (2025). The Digital Mirage: India's Evolving Legal Battle Against Deepfake Technology. *SCRIPTed: A Journal of Law, Technology & Society*, 22(2), 162-226.

¹⁵ Seth, N., Patel, N., & Jindal, R. (2024). Enhancing Resilience of Deepfake Detection using Adversarial Frequency Masking. *Grenze International Journal of Engineering & Technology (GIJET)*, 10.

¹⁶ Guruswamy, M. (2017). Justice KS Puttaswamy (Ret'd) and Anr v. union of India and Ors. *American Journal of International Law*, 111(4), 994-1000.

¹⁷ Birrer, A., & Just, N. (2025). What we know and don't know about deepfakes: An investigation into the state of the research and regulatory landscape. *New media & society*, 27(12), 6819-6838.

¹⁸ Buo, S. A. (2020). The emerging threats of deepfake attacks and countermeasures. *arXiv preprint arXiv:2012.07989*.

Westerlund, M. (2019)¹⁹ pointed out that presently the media phenomena are composite and blurring the distinction between actual and fake. Deepfakes are become a major concern, as they are hyper-realistic videos generated using artificial intelligence (AI) that make it seem as if someone has said or done something they didn't. The extensive reach and rapid dissemination of social media enable convincing deepfakes to swiftly impact millions, adversely affecting society. This study investigates publicly accessible internet news items to explore the nature of deepfakes, their producers, the advantages and risks associated with deepfake technology, notable examples, and strategies for combating deepfakes, despite the limited scholarly study on the subject.

Hasan, H. R., et al., (2019)²⁰ indicate that although deepfakes pose a considerable threat to society, the political framework, and commerce, can be mitigated through legislation and regulation, corporate policies and voluntary measures, education and training, alongside advancements in technology for deepfake detection, content authentication, and prevention. The study offers an extensive analysis of deepfakes and presents cybersecurity and AI entrepreneurs with potential prospects in combating media forgeries and misinformation. Gamage, D., et al., (2021)²¹ discussed the proliferation of Deepfake tools and technologies in the public domain is increasing. Scholarly study predominantly focuses on the technology of deepfakes, although is limited in its examination of the societal implications of their emergence. This systematic review examines scholarly works on deepfakes that emphasise societal ramifications rather than a technology-centric perspective.

Sharma, M., et al., (2021)²² concentrated on the counterfeit digital content circulated online has presented significant challenges for numerous social media platforms and real-world applications. Technological innovation has enabled the creation of material to the extent that distinguishing between false and factual information has become increasingly difficult. One emerging technique, termed deepfake, can generate hyper-realistic yet fraudulent content that is difficult for the human eye to detect and appears exceedingly authentic. The technology depends on artificial intelligence and its components, specifically machine learning and deep learning.

3. RESEARCH METHODOLOGY

This study employs a doctrinal and analytical methodology. The principal sources examined comprise the “Bharatiya Nyaya Sanhita, 2023,” the Information Technology Act, 2000, the Bharatiya Sakshya Adhiniyam, 2023, and pertinent subordinate legislation, including the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. Secondary materials comprise articles from Indian and International Law Journals, monographs on Cyber Law and AI governance and policy articles from various organisations. The methodology adopted was prescriptive, as the study has not only described the provisions in place but also evaluated the provisions based on the unique characteristics of deepfake technology, outlook forward with recommendations made on comparative best practices.

This analysis draws out what we can do, at present, and what needs to be done in the future through further legislation. The study relies on both primary and secondary sources to derive its findings, namely the Bharatiya Nyaya Sanhita, 2023, along with books, journals, official publications, and legal commentary. The critical analysis has been employed to evaluate the merits and flaws of the new law.

¹⁹ Westerlund, M. (2019). The emergence of deepfake technology: A review. *Technology innovation management review*, 9(11).

²⁰ Hasan, H. R., & Salah, K. 2019. Combating Deepfake Videos Using Blockchain and Smart Contracts. *IEEE Access*, 7: 41596–41606. <https://doi.org/10.1109/ACCESS.2019.2905689>.

²¹ Gamage, D., Sasahara, K., & Chen, J. (2021). The Emergence of Deepfakes and its Societal Implications: A Systematic Review. *TTO*, 1(1), 28-39.

²² Sharma, M., & Kaur, M. (2021). A review of Deepfake technology: an emerging AI threat. *Soft Computing for Security Applications: Proceedings of ICSCS 2021*, 605-619.

This qualitative study mostly relies on secondary sources to analyse the existing legal frameworks for deepfakes in the United States, the European Union, and India. This methodology facilitates an accurate evaluation of the adequacy of existing legislation and supports the study objective of proposing educated legal and policy suggestions to address the emerging difficulties posed by deepfake technology.

4. RESULTS

H₁: The existing legal framework under the Information Technology Act, 2000 is inadequate to effectively address emerging deepfake-related crimes in India.

The study analysed that the regulation of deepfake technology poses several technological and legal issues. These difficulties hinder the efficient governance and mitigation of hazards associated with deepfakes. Despite substantial advancements in deep fake detection systems, the evolving nature of deep fake creation remains a difficulty. An integrated strategy that incorporates machine learning, digital watermarking, and forensic analysis, alongside on-going study and adaptation, is crucial for effectively addressing the challenges presented by deep fake technologies²³. This study shows that the current regulatory regime of India is inadequate on issues surrounding deep fake technology. While there are some provisions for affordability under current regulations, they lack clarity and comprehensiveness to meet the unique issues of synthetic media. An examination of the enforcement environment shows the weaknesses in investigative powers, the efficiency of prosecution, and victim assistance mechanisms²⁴.

The Principal Dilemma: Free Expression Versus Veracity and Injury, as evidence of the impact of specific uses of deepfakes – particularly harmful, deceptive, and defamatory – continues to mount, the case law pointed to the need for caution and further debates about how to regulate the freedom of expression. While automated detection technologies and regulatory solutions might seem like solutions, they need to be considered in terms of their alignment with freedom of expression rights. In the study two overly-contrived solutions are often proposed and are quickly rejected. The first argument of the deepfakes not being protected by free speech is that they are artificial. This view overlooks the fact that not everything that is wrong is of little or no expressive content. Satire, satire, and art fiction often are both fictional elements and part of the public discourse. The second argument states that deepfakes should only be regulated if they are used to trick people into believing something that doesn't actually exist – something that a perfectly innocent synthetic video could do just as well²⁵.

H₂: The laws of the Bharatiya Nyaya Sanhita, 2023 offer stronger tools for combatting deepfakes offences.

The study significantly bolsters the idea and explored The Bharatiya Nyaya Sanhita, 2023 which broadens laws on identity misuse, impersonation, defamation, privacy violation, and cyber-crimes. There have been recent cases in court where judges have been aware of the harm being caused by deepfakes, especially in situations involving AI generated media concerning public individuals. Though the study does not specifically define or regulate deepfakes, it's important to note that the provisions of BNS, 2023 can offer a broader framework than existing laws for combating occasions of deepfakes or content manipulation. The need for targeted anti-deepfake law is evident.

²³Minhas, N. R., & Sonkhla, D. (2024). Exploring legal and technical challenges of deep fakes in India. *International Journal For Multidisciplinary Research*, 6(4).

²⁴ Kashyap, S. (2025). The Digital Mirage: India's Evolving Legal Battle Against Deepfake Technology. *SCRIPTed: A Journal of Law, Technology & Society*, 22(2), 162-226

²⁵ Schick, N. (2020). Deep fakes and the Infocalypse: What you urgently need to know. Conran Octopus

The study explored the shortfall in the present legal regime, which is rather weak and disjointed, and allows perpetrators of deepfake offenses to evade responsibility. The study must not rely on superficial remedies and not seek to address what is a fundamentally new problem by resorting to “old” law or “old” solutions²⁶.

To uphold the principles of respecting a fundamental right to privacy that was laid out in the Puttaswamy ruling, India must have a verbiage that attempts to put a cap on the making and spreading of deepfakes. The study recommended that this is the only remedy to correct the gaps and the best interests of the public. The legislation must have strong support systems in order to be effective. The restrictions to be put into place include mandatory watermarks on AI-generated text, real accountability of social media platforms and capable forensic experts to ensure that it is clear between genuine or fabricated information. Its basic premise is that it faces a technology that continues to improve no end. If committed to upholding the right to privacy established in the “Puttaswamy verdict”, India requires a definitive law governing the creation and dissemination of deepfakes. This is the sole method to close the gaps and ensure public safety. For the legislation to be effective, it requires strong support systems in place. Incorporating stipulations such as mandatory watermarks on AI-generated content, genuine accountability from social media platforms, and proficient forensic experts capable of differentiating between authentic and fabricated material. Fundamentally, competing with technology, which is increasingly proficient at replicating reality daily²⁷.

H₃: The absence of specific statutory provisions regulating deepfake technology creates challenges in investigation, prosecution, and victim protection.

The study pointed that the current legal framework is fragmented and inadequate, allowing perpetrators to escape prosecution for deepfake exploitation. The study cannot afford to fall back on palliatives, nor to try to enforce old statutes to meet a new crisis. Amongst the study's key findings is that the current legislation is lacking in its ability to keep pace with rapid technological advancements, which is the main problem. Existing laws and regulations are largely built prior to the advent of deepfakes as a key threat, and reflect the lack of recognition and consideration of the unique harms caused by human-altered, AI-generated digital manipulators²⁸.

Conventional privacy, defamation, identity fraud, and copyright theories from jurisdictions remain the main legal pillars to manage the classic unlawful uses of AI, rather than the high-tech uses and misuse of AI, which are the key issues that these theories struggle to answer. These traditional privacy, defamation, identity fraud and copyright theories are still being used to address typical uses and misuses of AI, not advanced technological applications using AI. The unique features of deep fake technology, including the ability to create hyperrealistic face and voice impressions, and its wide spread via social media, has created unprecedented challenges for the legal system which are presently not entirely answered. Potential novel developments could include changing the simulated to actual blockchain infrastructure to give greater confidence in immutability as well as adding an intuitive interface for forensic use and assessing use of the tool with real forensic case material²⁹.

H₄: An all-encompassing and technology-independent regulation is needed to properly counter and prevent deepfake crimes, while safeguarding freedom of expression and privacy rights.

²⁶ Bharatiya Sakshya Adhiniyam, No. 47 of 2023, section 2(e), 57,58 (India)

²⁷ Yadav, P. (2025). INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES. Available at SSRN 6549719

²⁸ Afshari, N., & Mohammadi, A. (2023). The legal implications of deepfake technology: Privacy, defamation, and the challenge of regulating synthetic media. *Legal Studies in Digital Age*, 2(2), 13-23

²⁹ Darma, M., Gisymar, N. A., Purwadi, A., Zubaedah, P. A., & Judijanto, L. (2025). Legal Implications of Deepfake Technology Misuse in Digital Content on Social Media. *Science of Law*, 3, 98-103.

The study revealed the direction in which India is going with on-going development of deepfake technology, to determine if the world's largest democracy can secure fundamental rights against such technology while also enabling technological innovation. Indeed, one of the main choices for policy makers is to take a leading role, in a coordinated manner, in developing the global governance framework of synthetic media – a field in which they can accept deeply regulating the system in order to keep the property rights of producers and the trust of users – or to witness epistemic confidence fading because users cannot tell the truthfulness from the artificiality of the content they consume. It is not just a technical problem calling for technical solutions, it is a challenge to existing laws, which had their origins in analogue environments, that will have to evolve in order to meet the threats posed in digital environments, such as to identity, to democratic discourse, to human dignity, and to life and existence on an algorithmic scale³⁰.

Article 19(1) (a) of the Constitution ensures the freedom of speech and expression for all people, contingent upon the limitations specified in Article 19(2) of the Constitution. Article 19(2) permits the State to impose reasonable limitations on the freedom of speech and expression for the purposes of safeguarding State security, maintaining the sovereignty and integrity of Bharat, fostering amicable relations with foreign nations, ensuring public order, upholding decency or morality, preventing contempt of Court, addressing defamation, and averting incitement to an offence. In *K.S. Puttaswamy v. Union of India*, the Supreme Court determined that the right to privacy is an inherent component of the right to life and liberty as provided by Article 21 of the Constitution, asserting that informational privacy is a significant aspect of the Right to Privacy. The Court noted³¹.

Furthermore, the study analysed that the governments should promote collaboration between technology specialists and legal professionals to develop effective, technology-informed regulatory frameworks that can adapt to on-going advancements in AI-driven content generation. Although deepfake technology offers significant prospects for the entertainment and educational industries, its abuse poses serious legal and ethical dilemmas, such as defamation, privacy violations, identity theft, and misinformation. Current laws in many jurisdictions fail to adequately address the challenges created by deepfakes due to their complexity, leading to uncertainty and challenges of implementation. Existing laws are usually not attuned to emerging technologies, and often are ambiguous in scope to respond to new forms of digital criminal activity³².

5. DISCUSSION

The rise of deepfakes brings challenging issues to all segments of society, such as the political realm, business, and personal lives of politicians and citizens alike. This paper (Rai, O. P. 2025)³³ discusses the various social implications of the deepfakes. The topics discussed are the Bharatiya Nyaya Sanhita (BNS), 2023, which has been touted as a pivotal change in the criminal justice system of post-Independent India and the evolution of the Indian judiciary. The law prevails over the Indian Penal Code (IPC) of 1860 which has been the basis of substantive criminal law for nearly 160 years. IPC was the bedrock of the criminal law in India but had many drawbacks such as colonial spirit, obsolete concept of crimes, failure to meet the needs of the modern society and constitutional framework.

³⁰ Kashyap, S. (2025). The Digital Mirage: India's Evolving Legal Battle Against Deepfake Technology. *SCRIPTed: A Journal of Law, Technology & Society*, 22(2), 162-226.

³¹ Regulation (EU) No 2016/679 of the European Parliament and of the Council of 27 April 2016 on protecting natural persons about the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union, L119, 1-88.

³² Verma, K. (2024). Digital deception: The impact of deepfakes on privacy rights. *Lex Scientia Law Review*, 8(2), 859–896.

³³ Rai, O. P. (2025). Criminal justice reforms in India: a critical study of the Bharatiya Nyaya Sanhita, 2023. *Journal of Advanced Education and Sciences*, 5(2), 88-93

(Chawla, R. 2019)³⁴ signifies that the aim of the Bharatiya Nyaya Sanhita to modernise the criminal law by restructuring and introducing new crimes as well as updating the definition of crimes according to the modern state of society and justice in measures of constitutional standards. This section critically evaluates the key changes recommended by the BNS and how these would affect the criminal justice system in India.

One of the key factors in these shortcomings highlighted by the study is the lack of technical expertise among lawyers in managing the technical complexities surrounding AI-induced manipulations. Judicial and regulatory bodies often lack technical expertise to properly assess the authenticity of deepfakes or the extent of manipulation, further fueling the significant delays and implementation challenges. (Syaidi, R., et al., 2022)³⁵ stated that the effectively mitigate the harm caused by the misuses of deepfake technology, it is crucial for the legal framework and process to include technological competency, as well as precisely and systematically rework regulatory regimes with clear definitions, accountability frameworks, and prompt responses. Lastly, there should be a lot of legal reform, such as precise definitions, improved regulations, dedicated training of legal units and closer cooperation with international teams, if we really want to be able to effectively fight the significant and gradually increasing threat of deepfake.

6. CONCLUSION

The study concluded that the deep fake technology which poses threat to individual privacy, their personal reputations and the democratic integrity is clearly showing that there is a huge loophole in Indian legal framework. Most of the existing laws, including the IT Act, 2000, and Bharatiya Nyaya Sanhita, are reactive and non-coordinated. They address only the downstream issues of defamation, fraud or obscenity after the damage is done, but don't explicitly criminalize the harm of the dangerous creation or intentional sharing of fake images. In the study, this situation of an absence of a statutory remedy is compounded by the difficulty of attribution, jurisdiction and intermediate responsibility. India needs a pro-active approach in the regulation of the new threat and move out of the reactive phase. It calls for a holistic approach with the adoption of a specific Deepfake Regulation Act to define and punish AI-related abuses, in updating existing cyber law with notions of synthetic identity and harm, and in recognizing digital personality rights to prevent identity theft. Some of the study's key findings are that improving the forensics skills, establishing strong platform accountability, and raising public awareness are both vital. Without more complete and up-to-date protections, citizens are at risk of being abused digitally, silently undermining the trust in the integrity of information and institutions.

While the study looks at the many benefits of the deepfake technology, the demand for its sophisticated skills makes many faux movies and images difficult to tell apart from their real counterparts. It can imitate both human actions and appearance, and provides the means to create convincing fake content, that may spread disinformation and hoaxes. When law doesn't explicitly mention the nefarious uses of deepfakes, it can cause lasting and extensive damage. Whilst current legislation covers a number of concerns raised in the study in relation to the malicious use of deepfakes, there is a compelling case for more in-depth legislation that ensures the protection of personal privacy and identity whilst respecting freedom of speech. Deepfakes have the potential to blur lines and without proper regulation could be used to accomplish negative goals. This highlights the need for comprehensive laws that cover every aspect of deepfakes, with a particular focus on their misuse and the potential consequences of such actions. "China's Deep Synthesis Technology

³⁴ Chawla, R. 2019. Deepfakes: How a pervert shook the world. *International Journal of Advance Research and Development*, 4(6): 4–8.

³⁵ Syaidi, R., & Budianto, A. (2022). Inner fingerprint check criminal action investigation. In *Proceedings of the 2nd International Conference on Law, Social Science, Economics, and Education (ICLSSEE 2022)* (p. 470). EAI.

Regulating Deepfake-Related Crimes in India: A Critical
Analysis of the Information Technology Act and Bharatiya
Nyaya Sanhita, 2023

Regulation” is a tough approach to this problem, with severe penalties for those who break the rules. The study reveals a challenge not just legal in nature, but entails a lot of moral questions as well. A well-regulated environment creates trust in the media, improves security at both a national and international level and could make the internet more secure, protecting human dignity.

The key takeaways from this research underscore the critical need for specific legislative solutions to address the multifaceted challenges Deepfakes pose. A legal or technological answer is insufficient — an interdisciplinary approach which ages the use of legal structures and skill in technology is required. To manage deep fake technology, we need a national strategy that involves multiple strategies together, including a genuine legal revision, technological advancements and teaching programs. All-round efforts to curb risks arising from deepfakes in India can be boosted by enacting suitable laws, coordination among nations, fortifying solutions for detection and enhancing awareness among the people. This holistic system would help to reduce misuse of deepfakes, respect citizens' rights and privacy and safeguard a safer digital world in the end.