INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

DEEPFAKE CRIMES AND CRIMINAL LIABILITY IN INDIA: A CRITICAL ANALYSIS UNDER BNS AND IT LAWS

AUTHORED BY - SAMRUDDHI JAISWAL
CO-AUTHOR - SUMIT TRIPATHI
Institution - G. H. Raisoni College Of Law Saikheda (M.P)

ABSTRACT

The development of deepfake technology relies heavily on the rapid progress of AI and machine learning technologies, allowing for the generation of incredibly realistic but fake audio, visual and video content. While deepfakes can be used for positive and creative purposes such as entertainment, education, and digital innovation, their negative applications have posed a significant threat to privacy, reputation, public order, electoral integrity, and national security. As the use of manipulated media has grown in India, through digital networks and social media, numerous forms of cybercrime have emerged, such as impersonation, identity theft, defamation, financial fraud, cyber harassment, non-consensual pornography, and misinformation campaigns. There are concerns around the criminal liability for deepfake crimes and how they are addressed, as there is no dedicated statute that targets deepfake crimes. The paper critically examines the legal parameters of addressing deepfake related offences under the Bharatiya Nyaya Sanhita, 2023 and Information Technology Act, 2000. It looks at the use of provisions on cheating by personation, forgery, defamation, obscenity, publication of sexually explicit material, identity theft and violation of privacy to deal with deepfake offences. The paper also discusses the issues of intermediary liability, digital evidence and forensic investigation in relation to the prosecution of such crimes. Judicial developments such as those considering privacy, free speech, intermediary responsibility and online harms have also been considered to address the developing legal landscape. It reveals that the current legislation is not robust enough to tackle technologically advanced crimes and calls for robust laws and law enforcement mechanisms and regulations to stop deepfake misuses in India.

KEYWORDS:

Deepfake Technology, Artificial Intelligence, Cybercrime, Criminal Liability, Bharatiya Nyaya Sanhita, Information Technology Act, Digital Evidence

ISSN: 2582-6433

INTRODUCTION

Technologies related to the development of artificial intelligence have changed the face of the digital world to the extent that it enables machines to replicate human speech, look and act like humans very realistically. A major issue with this technological feat is the rise of deepfake technology. Deepfakes come from "deep learning" and "fake," and are manipulated digital content created using artificial intelligence and machine learning. Deepfake technology involves the use of algorithms like Generative Adversarial Networks (GANs), which generate convincing and realistic fake audio, video, or images. While it is true that this technology has some valid uses in entertainment and education and even in healthcare and filmmaking, its misuse has been a big legal and social issue in the world.[1]

In the past few years, India has seen a surge in the utilization of deepfake technology via social media, messaging apps, and digital communication networks. Deepfakes are being used more and more to make fake political speeches, financial scams, cyber defrauding, impersonation, revenge pornography, online harassment and misinformation campaigns.[2] The deceptive manipulation of AI-generated deepfake videos, which have been circulating online and seen by thousands of people, clearly shows how easy it is for AI to create videos that are not true and to deceive the public.

The legal implications of deepfakes are multifaceted, as the legal framework in India is not explicitly geared towards regulating AI-generated content. There is no specific legislation that criminalizes specific offences caused by the use of deepfake technology other than provisions in the Bharatiya Nyaya Sanhita, 2023 and the Information Technology Act, 2000.Currently, multiple provisions in the Bharatiya Nyaya Sanhita, 2023, and the Information Technology Act, 2000 are applicable to offences committed by deep fake technology. There is yet no precise definition of deepfakes in any of these laws, and no procedures for detecting, investigating or prosecuting deepfakes.[3] This leaves huge loopholes in the laws that could lead to criminal liability in the event of an offence.

The judiciary has also served a key function as it has recognised digital privacy and online

[1] Ian Goodfellow, Yoshua Bengio and Aaron Courville, *Deep Learning* 526 (MIT Press, Massachusetts, 2016).
[2] Robert Chesney and Danielle Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security" 107 California Law Review 1753 (2019).
[3] The Bharatiya Nyaya Sanhita, 2023, ss. 318, 336, 356; The Information Technology Act, 2000 (Act 21 of 2000), ss. 66C, 66D, 67, 67A.

ISSN: 2582-6433

dignity as fundamental constitutional rights. This ruling has far-reaching consequences for various offences relating to deepfakes, such as unauthorized use of a person's image, voice or identity, under Article 21 of the Constitution of India, which the Supreme Court has classified as a fundamental right. Likewise, in Shreya Singhal v Union of India, the Supreme Court underscored the need for balancing freedom of speech with reasonable restrictions in the digital world.[4] The judicial statements give constitutional direction to combat the new cybercrime generated by the use of artificial intelligence and manipulated media.

Intermediary liability and digital governance are other significant hurdles of deep fake crimes. Dispersed social media platforms and online intermediaries can be the main source of the spread of manipulated content. The enforcement of due diligence on intermediaries under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 is lagging due to technological complexities and jurisdictional issues, and addition, the anonymous and borderless nature of cyberspace makes it difficult to identify and prosecute offenders.[5]

There are also significant evidentiary issues in the criminal justice system that must be addressed related to deep fake crimes. Manipulated media can look very authentic; investigation agencies have significant challenges in identifying authentic digital evidence from manipulated media. It's essential for advanced forensic mechanisms and specialized cyber investigation units to be developed to detect deepfakes that are AI-generated, otherwise the misuse of deepfake technology can create a lack of confidence in the justice system and digital evidence.[6]

Thus, the present study critically reviews the concept of deepfake crimes and examines the criminal liability of deepfake crimes as per the Bharatiya Nyaya Sanhita, 2023 and Information Technology Act, 2000. The paper aims to assess the current legal frameworks, judicial rulings, and enforcement strategies to determine their effectiveness in combating cybercrimes fueled by AI in India.

[44] *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.
[5] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, rr. 3, 4.
[6] Matthew Groh, Ziv Epstein, et.al., "Evaluating Deepfake Detection in Real-World Scenarios" *available at:* https://arxiv.org/abs/2202.07145 (last visited on May 29, 2026).

ISSN: 2582-6433

STATEMENT OF PROBLEM

With the advent of deepfakes technology, privacy, reputation, identity, and digital security are all facing serious issues in the Indian context. Using artificial intelligence and machine-learning techniques, deepfakes can generate highly realistic but fake audio, video and image content that could be used to mistakenly portray individuals engaging in actions or saying things that never actually happened. The wide-spread access to these technologies via social media and digital apps has greatly raised the danger of misuse in relation to crimes like cyber fraud, defamation, revenge pornography, financial scams, and political misinformation, among others. The proliferation of manipulated media in the viral media has not only impacted the individuals but also has challenged the consumer's trust of digital information and democratic processes.

However, while deepfake crimes are on the rise, there is no specific law in India that addresses only artificially generated manipulated content via AI. Currently, offences based on Deepfakes are dealt with through piecemeal laws in the Bharatiya Nyaya Sanhita, 2023 and the Information Technology Act, 2000 pertaining to cheating, forgery, identity theft, obscenity, defamation, and breach of privacy. These, however, were in place prior to the dawn of sophisticated artificial intelligence technologies and are thus not sufficiently robust to cover the offences in relation to deepfakes. There is no statutory definition of deepfakes, no clear guidelines on who can be held liable and a lack of guidance on how to investigate the crime and collect digital evidence.

Moreover, the proliferation of deepfakes on the Internet and social media platforms involves intricate issues regarding intermediary liability, freedom of speech, privacy and cyber governance. The complexity of AI tools presents challenges for investigating agencies in detecting and verifying manipulated digital content. The lack of proper mechanism to detect and protect the forgery, as well as comprehensive regulation, is a significant risk to cyber security, public order and criminal justice. Thus, it is a pressing need to critically analyze the status quo and propose the necessary changes to the law to tackle criminal liability in the context of deep fake crimes in India.

ISSN: 2582-6433

RESEARCH QUESTIONS

1. What is the nature and scope of deep fake technology and how it is being misused for criminal activities in India?
2. Whether the existing provisions of Bharatiya Nyaya Sanhita, 2023 and the Information Technology Act 2000 are suffice to deal with offences of deepfakes?
3. How do deepfake crimes affect implications for privacy, reputation, dignity and freedom of speech in the digital sphere in the context of deepfakes?
4. What are the mjor legal and technological challenges for investigating agencies and courts in the fight against deepfake crimes?
5. What are the legal reform and regulatory measures needed to effectively fight deepfake crimes and hold the criminal responsible in India?

RESEARCH OBJECTIVES

1. To explore concept, evolution and working of deep fake technology and its misuse in cyberspace.
2. To analyse the provisions of Bharatiya Nyaya Sanhita, 2023 and Information Technology Act, 2000 versus Deepfake crimes and criminal liability.
3. To examine the effects of deepfakes on privacy, reputation, digital security and constitutional rights.
4. To evaluate the function of courts, investigating agencies and intermediaries in tackling deepfake crimes in India.
5. To suggest the necessary legal, regulatory and policy changes for the prevention and control of deep fake crimes in India.

HYPOTHESIS

The current legal framework, as captured in the Bharatiya Nyaya Sanhita, 2023 and Information Technology Act, 2000 lacks the specific statutory provisions, technological readiness, and enforcement capabilities to effectively regulate and prevent crimes related to deepfakes in India, further emphasizing the need for dedicated legal and regulatory reforms to tackle criminal liability linked to deepfake misuse of AI-generated content.

ISSN: 2582-6433

LITERATURE REVIEW

Ian Goodfellow, Yoshua Bengio and Aaron Courville in their book Deep Learning explain the technological foundations of artificial intelligence and machine learning, particularly the functioning of neural networks and Generative Adversarial Networks (GANs), which are widely used in the creation of deepfake content.[7] The book provides a detailed understanding of how synthetic media is generated and manipulated through advanced algorithms, thereby helping in understanding the technical basis of deepfake crimes.

In Artificial Intelligence: A Modern Approach, Stuart Russell and Peter Norvig explore the history, uses, and threats of the technologies of artificial intelligence and raise ethical and legal issues related to artificial intelligence, such as the potential for automated technologies to be misused for deceptive and cyber purposes.[8]

In Cyber Crimes, Talat Fatima explains different types of cybercrimes in Indian law and explores the legal regulation of cybercrime under the Information Technology Act, 2000, which are especially pertinent when considering the criminal aspects of the deepfakes.[9]

While addressing the issues related to privacy, cyber security and electronic evidence, the book does not focus on deepfake related offences, indicating the need for more research on this topic. Aparna Viswanathan in Cyber Law: Indian and International Perspectives on Key Topics Including Data Security, E-Commerce, Cloud Computing and Cyber Crimes discusses the evolving contours of ‘cyber law' and ‘digital governance'.[10]

In their article, Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, Robert Chesney and Danielle Citron criticize the potential threats of deepfakes to democratic institutions, public trust and individual privacy, and call for more robust legislation to address those risks.[11]

[7] Ian Goodfellow, Yoshua Bengio and Aaron Courville, *Deep Learning* 526 (MIT Press, Massachusetts, 2016).
[8] Stuart Russell and Peter Norvig, *Artificial Intelligence: A Modern Approach* 2 (Pearson Education, London, 4th edn., 2021).
[9] Talat Fatima, *Cyber Crimes* 115 (Eastern Book Company, Lucknow, 2016).
[10] Aparna Viswanathan, *Cyber Law: Indian and International Perspectives on Key Topics Including Data Security, E-Commerce, Cloud Computing and Cyber Crimes* 210 (LexisNexis, Gurgaon, 2012).
[11] Robert Chesney and Danielle Citron, “Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security” 107 California Law Review 1753 (2019).

ISSN: 2582-6433

In "Pornographic Deepfakes: The Case for Federal Criminalization," Rebecca A. Delfino outlines the psychological, reputational, and social harm that victims of deepfakes suffer as well as the criminalization of those who create and disseminate such pornography.[12]

In her article, Deepfakes and the Emerging Challenges to Data Protection and Privacy in India, Swati Srivastava looks at the limitations of cyber laws in India and the need for protection of data and enhanced digital privacy protection.[13]

The issue of manipulated digital media has been recognised by various scholarly publications relating to cyber law and artificial intelligence, and the current legal systems are not sufficient to address the problem. These scholarly articles in the Indian Journal of Law & Technology have collectively highlighted that the current legal regime is inadequate to deal with tech-enabled crimes involving AI-generated content.[14]

Likewise, various international journals like the California Law Review and the Boston University Journal of Science and Technology Law have written extensively about the impact of deepfake technology on notions of privacy, democracy, cybersecurity, and freedom of expression.[15]These journal articles offer comparative perspectives and insights into the regulatory challenges and potential legal solutions to the problem of deepfake offences.

The use of AI and cyber manipulation is also a growing threat, with government and institutional reports acknowledging the potential dangers. The spreading of manipulated and misleading contents on social media platforms has been repeatedly reported and has been highlighted as a matter of concern in the context of cybersecurity and intermediary regulation by the Government of India through the Ministry of Electronics and Information Technology.[16] The dangers of deep fakes are also recognised by international organisations and research institutions. Overall, the reports highlight the importance of having robust multijurisdictional legal frameworks to effectively address deepfakes for criminal liability, and the need for

[12] Rebecca A. Delfino, "Pornographic Deepfakes: The Case for Federal Criminalization" 13 Boston University Journal of Science and Technology Law 1 (2019).
[13] Swati Srivastava, "Deepfakes and the Emerging Challenges to Data Protection and Privacy in India" 5 Indian Journal of Law and Technology 44 (2021).
[14] See generally, *Indian Journal of Law and Technology*, available at: https://ijlt.in/ (last visited on May 29, 2026).
[15] See generally, *California Law Review* and *Boston University Journal of Science and Technology Law*.
[16] Government of India, "Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021" (Ministry of Electronics and Information Technology, 2021).

ISSN: 2582-6433

advanced forensic tools and greater intermediary obligations.[17]

RESEARCH GAP

In the current literature, AI technologies and cybercrime are mainly discussed in relation to privacy and misinformation issues, data protection and ethical problems associated with deep fakes. But there is not much extensive study, which has specifically focused on the criminal liability for the crimes arising out of deepfakes under the provisions of Bharatiya Nyaya Sanhita, 2023 and Information Technology Act, 2000. The majority of studies focus on the technological or policy aspects of deepfakes, rather than critically assessing the adequacy of the existing Indian criminal laws, intermediary liability, evidentiary issues and enforcement frameworks. Hence, the purpose of the present study is to add to this lacuna by conducting an exhaustive legal analysis of deepfake crimes and the efficacy of the existing Indian legal framework to tackle technologically advanced crimes.

RESEARCH METHODOLOGY

In this study, doctrinal research method is applied. Primary and secondary legal sources are analyzed qualitatively to give insights into the legal aspects and criminal liability of deepfake crimes in India. The main sources are the Information Technology Act, 2000, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, constitutional provisions, and various judicial interpretations given by the Supreme Court and High Courts on the subject of privacy, cybercrime, intermediary liability, freedom of speech, and digital evidence. The study also delves into the legal principles that govern cyber offences, identity theft, defamation, obscenity, forgery and misuse of artificially generated content.

Secondary sources are books, journal articles, research articles, reports, commentaries, online databases, and scholarly articles covering the subjects of AI, cyber law, privacy rights, and digital governance. A critical analysis of the relevant national and international literature has been conducted to grasp the new challenges arising from deepfake technology and the legal framework so far. The study is analytical and critical in nature and assesses the efficacy of the existing legislations in India in dealing with deepfake related crime and the need for reform in the existing laws. The study also seeks to recommend appropriate legal and regulatory

[17] World Economic Forum, "Global Risks Report" available at: https://www.weforum.org/ (last visited on May 29, 2026).

ISSN: 2582-6433

framework to further strengthen the criminal liability and enforcement framework of deepfake crimes in India.

DISCUSSION

The AI revolution has had a profound impact on digital communication and content creation, worldwide. The most controversial advancement in this area is the deepfake technology, which involves AI and deep learning to produce altered audio, video, and image content that often seems real. With the advent of readily available AI tools and social media platforms, deepfake-related crimes and manipulations in India have been spreading at an unprecedented pace, posing significant threats to privacy, cybersecurity, public trust, and democratic governance.[18] The deepfake technology is being misused for making fake political speeches, impersonation videos, financial scams, revenge pornography, cyber harassment and misinformation campaigns. Over the last few years, many deepfake videos of celebrities, politicians and journalists have been widely shared on social media platforms, causing confusion and outrage. The case of manipulated videos of actress Rashmika Mandanna, which allegedly involved the use of artificial intelligence technology to digitally superimpose her face onto a different person's body was one of the most popular incidents in India, sparking a lot of discussion about the issue of digital privacy, the safety of women and the need for better cyber regulation.[19] Likewise, false videos and artificial speeches of politicians during election seasons have been a cause for concern on issues of electoral manipulation and misinformation.

What is problematic about deepfakes is their potential for misuse, both legally and constitutionally. Though identity theft, cheating by personation, forgery, defamation, obscenity, and publication of sexually explicit material are all covered in the existing laws in India such as Bharatiya Nyaya Sanhita, 2023 and Information Technology Act, 2000, none of them were explicitly made for the regulation of AI generated manipulated content. [20]This makes it challenging for investigators and courts to prove criminality and gather accurate digital evidence in deepfake cases.

The use of AI to create a fake likeness, voice, or image of an individual can lead to devastating

[18] Robert Chesney and Danielle Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security" 107 California Law Review 1753 (2019).
[19] "Rashmika Mandanna Deepfake Video Sparks Debate on AI Misuse" *The Hindu*, Nov. 07, 2023.
[20] The Bharatiya Nyaya Sanhita, 2023, ss. 318, 336, 356; The Information Technology Act, 2000 (Act 21 of 2000), ss. 66C, 66D, 67, 67A.

ISSN: 2582-6433

psychological, social, and reputational consequences as it directly infringes upon several constitutional rights, including the right to privacy, dignity, and reputation guaranteed by Article 21 of the Indian Constitution. Women are especially vulnerable to deepfakes pornography and online exploitation, which has become the growing cyber-threats around the world. [21]The anonymity and borderless aspects of cyberspace also makes enforcement and prosecution more challenging, particularly where such content can be rapidly shared through social media platforms.

The question of intermediary liability and the digital governance is another significant question. Social Media businesses and online platforms are sometimes made means of the dissemination of manipulated material. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 contain provisions of 'DUE DILIGENCE" for intermediaries but it is still a challenge for the same due to technological constraints and the absence of timely detection mechanisms.[22]

ANALYSIS

In today's digital age, deepfake has become one of the most perilous implications of AI and digital manipulation. The deepfakes can generate fake audio, video and image content using machine learning algorithms and artificial intelligence tools that look authentic and convincing. The technology itself is not necessarily prohibited, and can be employed in good ways like filmmaking, education, entertainment, and digital innovation; however, its misuse has raised a host of serious legal and ethical and social issues. With the rise in AI applications and social media platforms in India, the deepfake technology has been utilized for impersonation, cyber fraud, misinformation, revenge pornography, and political propaganda among the various criminal activities.

One of the areas where deepfake crimes are problematic is the lack of existing legislation. Deepfake technology is not explicitly defined or governed in the Bharatiya Nyaya Sanhita, 2023 or Information Technology Act, 2000. These laws offer some form of protection for offences committed with the help of deepfakes, but are too vague and general to meet the technical challenges and evolving nature of AI-enabled crimes. Lack of a clear statutory

[21] *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.
[22] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, rr. 3, 4.

ISSN: 2582-6433

definition means that there is ambiguity about the scope of criminal liability and the enforcement.

The abuse of deepfakes also triggers significant constitutional issues regarding privacy, dignity and freedom of expression. Manipulated AI-generated content that isn't your own can have a significant impact on a person's reputation and mental health, especially when used to produce something sexual which they've not consented to or defamatory material. The Supreme Court in Justice K.S. Puttaswamy v Union of India has declared privacy as a fundamental right to every human being under Article 21 of the Constitution of India, and DeepFake misuse breaches this right by using a person's image, voice, or identity without their consent. However, balancing the constitutional rights to freedom of speech and expression guaranteed in Article 19(1)(a) should also be considered, particularly when deepfakes are created for satirical, parodial, artistic or other purposes.

The other major issue is how intermediaries and social media play a role in the dissemination of deepfakes. Social media apps can proliferate fake material among millions of users in a matter of moments. The anonymity of cyberspace and technological challenges of identification and detection of harmful content further hinder enforcement of the Rules, 2021. The criminal justice system also faces obvious challenges with respect to evidence and investigation in a deepfake crime. The difficulty in verifying the authenticity of evidence in the face of the seemingly authentic nature of deepfake content makes it challenging for investigating agencies. The absence of sophisticated forensic facilities and skill in cyber investigation puts law enforcement unable to run a successful investigation. Thus, a need for specialized forensic tools, cyber expert skills and regulatory frameworks to effectively tackle deepfake-related offences has emerged.

In this way, deepfake technology poses a grave risk to cyber security, public trust and constitutional order in India. As the widespread adoption of AI-generated content continues, the need for robust laws, greater intermediary responsibility, technological readiness, and robust enforcement frameworks to guarantee criminal punishment and individuals' protection from digital exploitation has become even more clear.

ISSN: 2582-6433

SCOPE OF THE STUDY

In this paper, an attempt is made to understand the concept of deepfake, its misuse and implications for law in India with specific reference to the Bharatiya Nyaya Sanhita, 2023 and Information Technology Act, 2000. The study centres on the different types of offences related to deepfakes including impersonation, identity theft, cyber fraud, defamation, misinformation, revenge pornography and the publication, sharing or dissemination of manipulated digital content via online platforms. It examines the current status of crimes created by artificial intelligence and reviews how existing criminal and cyber laws can be applied to these offences and the significance of intermediary liability, digital evidence and cyber forensic investigation for the resolution of these crimes. The research also examines constitutional issues concerning privacy, dignity, reputation and freedom of expression in the context of a misuse of deepfake technology. Existing judicial rulings, statutes, reports and scholarly articles have been reviewed to gain insight into the gaps and difficulties associated with the current legal structure and judicial and investigating processes. The study also aims to recommend law and policy changes to enhance cyber governance and hold perpetrators of deepfakes accountable in India.

LIMITATIONS OF THE STUDY

The study covers only doctrinal analysis of laws, judicial decisions, reports, and secondary materials on deep fake crimes and criminal liability in India. It does not require empirical studies, field surveys, interviews or statistical analysis of the practical implementation of laws or public opinion on the use of deepfake technology. The research is primarily focused on the BNS, 2023, and the ITA, 2000 and thus has limited scope of performing an extensive comparative analysis of the foreign legal systems governing the regulation of deepfake content. The developments of law and technology since this study was completed could impact on the validity of some observations and findings. Moreover, there are few precedents in India that address deepfake offences, thus the analysis is partly based on general principles of cyber law, privacy rights, intermediary liability and digital governance.

CONCLUSION

Deepfake technology has posed a significant issue of privacy, cybersecurity, reputation, and digital governance in India. While artificial intelligence can be used for a wide range of beneficial purposes, it has also been abused in impersonation, cyber fraud, misinformation, revenge pornography, and defamation, leading to serious legal and ethical issues. While there

ISSN: 2582-6433

are some remedies for such crimes in Bharatiya Nyaya Sanhita, 2023, and the Information Technology Act, 2000, the lack of specific laws to address deepfake crimes leaves gaps in the law and in practice.

The study points to the lack of effective legal frameworks to address technologically sophisticated forms of AI-offences. Other issues such as intermediary liability, electronic evidence and cyber investigation compound enforcement difficulties. Deepfake misuse also impacts constitutional rights like privacy, dignity and freedom of speech and calls for a balanced legal response. Thus, robust laws, cyber forensic capabilities, intermediary liability and appropriate regulation protection are imperative to address deepfake crimes and hold criminals accountable in the digital era.

REFERENCES

Books

1. Aparna Viswanathan, *Cyber Law: Indian and International Perspectives on Key Topics Including Data Security, E-Commerce, Cloud Computing and Cyber Crimes* (LexisNexis, Gurgaon, 2012).
2. Ian Goodfellow, Yoshua Bengio and Aaron Courville, *Deep Learning* (MIT Press, Massachusetts, 2016).
3. Stuart Russell and Peter Norvig, *Artificial Intelligence: A Modern Approach* (Pearson Education, London, 4th edn., 2021).
4. Talat Fatima, *Cyber Crimes* (Eastern Book Company, Lucknow, 2016).

Articles and Journals

1. Rebecca A. Delfino, "Pornographic Deepfakes: The Case for Federal Criminalization" 13 Boston University Journal of Science and Technology Law 1 (2019).
2. Robert Chesney and Danielle Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security" 107 California Law Review 1753 (2019).
3. Swati Srivastava, "Deepfakes and the Emerging Challenges to Data Protection and Privacy in India" 5 Indian Journal of Law and Technology 44 (2021).

Cases

1. *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.
2. *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

ISSN: 2582-6433

Statutes and Rules

1. The Bharatiya Nyaya Sanhita, 2023.
2. The Information Technology Act, 2000 (Act 21 of 2000).
3. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

Reports and Web Sources

1. Government of India, "Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021" (Ministry of Electronics and Information Technology, 2021).
2. Matthew Groh, Ziv Epstein, et.al., "Evaluating Deepfake Detection in Real-World Scenarios" available at: https://arxiv.org/abs/2202.07145 (last visited on May 29, 2026).
3. "Rashmika Mandanna Deepfake Video Sparks Debate on AI Misuse" *The Hindu*, Nov. 07, 2023.
4. World Economic Forum, "Global Risks Report" available at: https://www.weforum.org/ (last visited on May 29, 2026).