

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS



Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Managing Editor of IJLRA. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of IJLRA.

Though every effort has been made to ensure that the information in Volume II Issue 7 is accurate and appropriately cited/referenced, neither the Editorial Board nor IJLRA shall be held liable or responsible in any manner whatsoever for any consequences for any action taken by anyone on the basis of information in the Journal.

Copyright © International Journal for Legal Research & Analysis

EDITORIAL TEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board



Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.



Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India. India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi. (2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020). Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi. Formerly Assistant professor of Law, Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8 Articles in various reputed Law Journals. Conducted 1 Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration. 10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.



Avinash Kumar



Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship. He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi. Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi. He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS
ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

ARTIFICIAL INTELLIGENCE AND CRIMINAL RESPONSIBILITY: LEGAL CHALLENGES AND IMPLICATIONS FOR DEFAMATION IN INDIA

AUTHORED BY: POOJA RAJEEP

School of Law

CHRIST (Deemed to be University), Bangalore

Abstract

Deepfake technology, which represents a sophisticated application of artificial intelligence, facilitates the generation of exceedingly realistic synthetic media, encompassing images, audio, and video. While advantageous in realms such as entertainment, education, and healthcare, its improper use gives rise to ethical, legal, and security issues, including defamation, identity theft, misinformation, privacy infringements, and cyberbullying. The increasing complexity of deepfake technology complicates both detection and regulation, thereby necessitating robust legal and technical measures.

India's legal framework governing deepfakes continues to be disjointed. Current legislation, such as the Information Technology Act of 2000, the Indian Penal Code, and the BNS Act, provides only limited protection and lacks definitive regulations pertaining to the creation and dissemination of deepfakes. This study investigates deficiencies in privacy safeguards, the enforcement of cybercrime provisions, and defamation statutes, emphasizing the difficulties in prosecution stemming from ambiguous legal terminology.

Employing a qualitative and doctrinal methodology, this research scrutinizes legal statutes, judicial decisions, and expert opinions. It delves into ethical dilemmas and assesses the efficacy of AI-driven authentication and forensic methodologies for the purpose of detection. The study advocates the establishment of a comprehensive legal framework that incorporates more stringent laws, enhanced enforcement mechanisms, and obligatory AI detection systems. Fortifying legal provisions, enforcing AI regulations, and heightening public awareness are essential steps for alleviating the risks posed by deepfakes while ensuring the responsible utilization of artificial intelligence.

Introduction

The term Deepfake was familiarised in the year of 2017, which introduced the conception of Synthetic digital content. Deepfake is a particular application of Artificial intelligence, with deep AI-driven learning as a version of machine learning technology. It creates highly realistic fake images, audio, or any videos that are usually used for entertainment but are being misused.¹ They also raise concerns about the conduct of fraud and misrepresentation. An exemplar of deepfake learning can be face-swapping, when a person's face is replaced with another one using artificial intelligence technology.²

This technology creates lifelike images, video, and audio, by altering one's face and voice using the deepfake technology which will have the originality feeling by making the AI-generated content appear highly realistic and authentic. AI can generate content of people saying or doing things they never did or said before. Face motion transfer, synthetic face creation, deepfake face overlay, and voice cloning are some of the deepfake techniques.

The benefits of AI are spread into various industries, AI improves task accomplishment and efficiency. In health care. AI improves patient care through advanced diagnostics, imaging assistance, and improved personalized treatment plans. Realistic visual effects and automatic dubbing, as well as content personalization, are some of the ways that AI is used to sharper user experiences in the entertainment industry. In education, AI-powered simulations. Virtual tutors and language teaching programs make learning complex concepts easier and enhance engagement.

Even with all these benefits, deepfakes have become a new source of defamation, misuse, theft identification, privacy violation, and cyberbullying.³ It is becoming easier to create deepfake content with advanced deepfake technology and is more difficult to detect it. The spreading of synthetic fake made digital content can be manipulated political content or pornography, which can lead to a person's defamation which is made without their permission.⁴

¹ Kingra, S., Aggarwal, N. and Kaur, N. (2022). Emergence Of Deep-fakes And Video Tampering Detection Approaches: A Survey. *Multimedia Tools and Applications*.

² Irean Cucilovic, *Deepfake Technology - Criminal Law Implications*, 2024 CRIMEN 325 (2024).

³ Marina Aleksandrovna Efremova & Evgeniy Aleksandrovich Russkevich, *Deepfake and Criminal Law*, 2024 BULL. KAZAN L. INST. MIA RUSS. 97 (2024).

⁴ Catharine A. MacKinnon, *Pornography as Defamation and Discrimination*, 71 B.U. L. REV. 793 (November 1991).

Most of the available literature emphasizes the engineering problems of deepfake detection more than the ethical and legal aspects of deepfake in India. This paper will conclude the detailed study of the existing legal regulation on deepfake in India and bring its connection to defamation, by identifying the probable gaps in the regulations. The increasing danger by crimes related to deepfakes demands immediate legal actions with punishments by ethical and legal actions to minimize irresponsible behavior and damages.

Methodology

A combination of a focus on secondary data sources, this study takes a qualitative research technique. The secondary material consists of pertinent Indian legislation, rules, and court rulings. The research also benefited from the perspectives of technology law specialists and solicitors. The study used a doctrinal research approach, heavily referencing existing literature, including reports, policies, legal regulations, and authoritative sources, including official publications from regulatory authorities. In order to achieve the study goals, relevant legal frameworks, academic publications, and published works were found and examined using a desk-based research approach.

1. Connection to Legal Aspects

The legal ramifications of deepfake technology, especially in relation to criminal liability, warrant thorough examination. In Indian law, foundational concepts such as mens rea (guilty mind) and actus reus (guilty act) underpin criminal accountability.⁵ However, the application of these principles to autonomous AI systems poses considerable difficulties. The inquiry into whether AI can exhibit criminal intent or be held accountable for illegal actions necessitates a review of AI's legal status and associated ethical issues.

In India, defamation laws, particularly those outlined in Section 499 of the Indian Penal Code (IPC) and Section 356 of the Bharatiya Nyaya Sanhita (BNS) Act, are pertinent to content generated by AI that may be defamatory.⁶ The significance of intent in defamation cases is paramount; however, establishing intent becomes problematic when addressing autonomous AI systems.⁷ The emergence of deepfakes, which can produce damaging content independently

⁵ D. Nicholas Allen, *Deepfake Fight: AI-Powered Disinformation and Perfidy under the Geneva Conventions*, 3 NOTRE DAME J. ON EMERGING TECH. 1 (November 2022).

⁶ *Bharatiya Nyaya Sanhita*, 2023

⁷ Madhura Thombre, *Deconstructing Deepfake: Tracking Legal Implications and Challenges*, 4 INT'L J.L. MGMT. & HUMAN. 2267 (2021).

of human oversight, further complicates the conventional interpretation of intent in defamation matters.⁸

2. Challenges in regulating deepfakes under existing Indian laws

The Indian government is increasingly acknowledging the significant threat that deep-fakes pose and their extensive implications across various areas of society. As India advances in technology, the spread of deep-fake technology represents a major challenge, raising issues regarding privacy, misinformation, and cybercrime. Although the risks are escalating, India presently lacks a specific legal framework to effectively address deep-fakes in a comprehensive manner. Instead, it depends on existing legislation such as the Information Technology Act, 2000 (IT Act), complemented by sections from the Indian Penal Code, 1860 (IPC). Nonetheless, with the implementation of the Bharatiya Nyaya Sanhita (BNS) starting July 1, 2024, the legal landscape has changed, requiring a reevaluation of the regulation of deep-fakes.⁹ While the NITI Aayog's National Strategy for Artificial Intelligence (NSAI) in 2018 provided a general structure for the responsible application of AI, it does not sufficiently tackle the intricate challenges that deep-fakes present in today's digital landscape.¹⁰ A framework established in 2019 is inadequate to address the swiftly changing threats that deep-fake technology currently poses. Existing legislation, like Section 66E of the IT Act, penalizes the unauthorized recording, publishing, or transmitting of an individual's images via electronic media, with penalties of imprisonment or a fine (imprisonment for three years or fine of ₹2 lakh). In a similar vein, Section 66D criminalizes identity fraud executed through digital means, subjecting offenders to imprisonment of up to three years and a fine of ₹1 lakh. Regardless of these laws, deep-fake technology calls for more robust and focused legislation.¹¹

The regulatory framework overseeing deep-fake-related cybercrimes in India is fragmented and inadequate. Although multiple laws address deep-fake-related offences, they do not fully encompass the issue. The IT Act and its Intermediary Rules of 2021 impose specific responsibilities on platforms to eliminate misinformation, yet the enforcement mechanisms are weak. Additional legal frameworks such as the Indian Copyright Act, the Digital Personal Data

⁸ Knox-Mawer, R. "Defamation: Some Indian Precedents and the Common Law." *The International and Comparative Law Quarterly*, vol. 5, no. 2, 1956, pp. 282–85. *JSTOR*

⁹ Indian Penal Code, 1860

¹⁰ Vig, Shinu. "Regulating Deepfakes: An Indian Perspective." *Journal of Strategic Security*, vol. 17, no. 3, 2024, pp. 70–93. *JSTOR*

¹¹ Information Technology Act, 2000

Protection Act, the Protection of Children from Sexual Offences (POCSO) Act, and the Indecent Representation of Women (Prevention) Act provide some level of protection against particular kinds of deep-fake abuse. Nonetheless, India has yet to experience a significant legal case that explicitly establishes the legal boundaries concerning deep-fakes. The lack of clear legislation complicates enforcement, creating gaps in the regulatory framework.

Deep-fakes represent a distinct danger as they can be weaponized to carry out various cybercrimes. One of the most considerable dangers is identity theft and virtual forgery, where deep-fake technology is employed to generate false identities, alter public perception, and harm reputations. Sections 66C and 66D of the IT Act, alongside Sections 420 and 468 of the BNS (previously IPC), can be utilized to prosecute such crimes, but legal experts contend that more specialized laws are essential to effectively deal with the sophisticated nature of deep-fake fraud. Another concerning application of deep-fakes is the dissemination of misinformation to undermine governments, incite violence, or manipulate electoral processes. Sections 66F of the IT Act and provisions of the Representation of the People Act, 1951, can be invoked to prosecute offenders, but enforcement continues to pose a challenge.

Beyond political exploitation, deep-fakes are increasingly utilized for hate speech, online defamation, and violations of privacy. Sections 499 and 153A of the BNS, along with provisions under the IT Act, provide some legal options, but they are not specifically tailored to address AI-generated fabricated content. A particularly alarming factor is the exploitation of deep-fakes to produce non-consensual pornographic material, which can lead to severe repercussions for the victims.¹² Sections 67, 67A, and 67B of the IT Act, in conjunction with the POCSO Act and other obscenity regulations, offer some level of protection, yet enforcement is often inconsistent.¹³

In light of the escalating misuse of deep-fakes, India requires a more robust legal framework that is specifically designed to govern and penalize the malicious application of this technology. Although the government has initiated certain actions, such as issuing advisories to intermediaries and proposing changes to the IT Rules, these initiatives do not provide a comprehensive legal remedy. The intricate nature of deep-fake offenses necessitates a multi-faceted strategy that encompasses tougher laws, improved enforcement mechanisms, and

¹² *Id* Pg. 5, Note 7

¹³ The Protection of Children from Sexual Offences Act, 2012

heightened public awareness. The continuously evolving character of AI-generated content makes it crucial for lawmakers to respond rapidly in crafting legislation that directly confronts the deep-fake threat.

3. Infringement of Privacy, Obscenity, and Pornographic Content

Deepfake technology presents a considerable risk to individual privacy by generating altered images or videos that inaccurately portray people in compromising scenarios. These digitally modified materials can inflict significant harm on a person's reputation, disseminate false information, and lead to breaches of privacy. A primary concern is the unauthorized application of deepfake technology in pornography, where individuals' faces are superimposed onto explicit material without their consent. This form of misuse not only causes emotional trauma for the victims but also raises profound ethical and legal dilemmas. Indian legislation encompasses various provisions that address these infringements.¹⁴ The Information Technology Act of 2000 includes pertinent sections such as Section 66-E (penalties for privacy violations), Section 67 (penalties for the publication or transmission of obscene material in electronic formats), Section 67-A (penalties for the publication or transmission of sexually explicit content), and Section 67-B (penalties for the publication or transmission of child pornography). Furthermore, the Indian Penal Code of 1860, specifically Sections 292 and 294, imposes penalties for the sale and distribution of obscene materials. The Protection of Children from Sexual Offences (POCSO) Act of 2012 also contains Sections 13, 14, and 15, which specifically address the exploitation of minors in digital media.

4. Cyberbullying and Harassment

The exploitation of deepfake technology transcends privacy infringements, extending into targeted harassment and cyberbullying. Malicious individuals create deepfake videos or images to impersonate others, disseminating false information that can defame or humiliate the victims. A significant number of deepfake manipulations involve non-consensual pornographic content, disproportionately impacting women.¹⁵ The emergence of deepfake pornography, which initially gained traction on online platforms such as Reddit, has led to severe social and psychological repercussions for victims, including public humiliation, damage to reputation, and emotional distress.

¹⁴ Olga Jurasz & Kim Barker, *Sexual Violence in the Digital Age: A Criminal Law Conundrum?*, 22 GERMAN L.J. 784 (August 2021).

¹⁵ Smith, Hannah, and Katherine Mansted. "What's a Deep Fake?" *Weaponised Deep Fakes: National Security and Democracy*, Australian Strategic Policy Institute, 2020, pp. 05–10. JSTOR

Cyberbullying based on deepfakes has occasionally targeted public leaders and celebrities. Actors and well-known individuals whose photos were altered and used without their permission are notable examples.

5. Gaps in Indian Law Regarding Deepfakes

India does not have a distinct legal framework that explicitly defines and penalizes the creation, distribution, or misuse of deepfakes. The existing laws only address offenses related to deepfakes indirectly, resulting in ambiguity and ineffective enforcement. There is no legal definition of "deepfake" within Indian law, complicating the distinction between malicious deepfakes used for fraud or misinformation and innocuous ones created for satire or entertainment. In the absence of a clear definition, law enforcement encounters difficulties in classifying and prosecuting crimes associated with deepfakes. Current laws primarily emphasize the ramifications of deepfakes, such as fraud, identity theft, or defamation, yet do not criminalize the act of creating and disseminating deepfake content itself. Other countries have enacted laws that directly penalize the production of deepfakes, a measure that India has yet to adopt.

While digital platforms are obligated to remove harmful content, there are no stringent penalties for not regulating deepfakes. Furthermore, India does not require AI detection tools or watermarking mandates for technology companies to identify or label deepfake content. This limitation weakens the capability to monitor and mitigate the proliferation of such media, complicating enforcement efforts. Indian law also fails to explicitly address explicit content generated by deepfakes. Although certain laws offer partial protection, they do not encompass instances where AI-generated images or videos are utilized to manipulate an individual's likeness. Victims encounter considerable obstacles in pursuing justice due to the anonymity of offenders and the absence of robust digital forensic mechanisms.

The lack of a specific deepfake law results in gaps in addressing the evolving threats presented by AI-generated content. As deepfake technology continues to develop, India necessitates a more comprehensive legal framework that criminalizes both the creation and dissemination of harmful deepfakes.¹⁶ Enhancing enforcement mechanisms, instituting AI detection regulations, and ensuring stricter accountability for digital platforms are crucial measures to address the

¹⁶ A. Amarendar Reddy, *Human Rights vs Artificial Intelligence*, 4 INDIAN J.L. & LEGAL RSCH. 1 (2022).

escalating risks associated with the misuse of deepfakes.

6. Ethical Boundaries in Deepfake Production Approaches and Technological Remedies

The current methods for detecting deepfakes mainly concentrate on spotting small imperfections caused by manipulation algorithms, such as boundary artifacts, shading inconsistencies, or unnatural facial characteristics. Nevertheless, with ongoing advancements in AI technology, the vulnerabilities of today may transform into strengths, rendering detection more difficult. Realizing a forensic technology that can definitely differentiate between genuine and manipulated content remains an enduring objective. To combat the misleading capabilities of deepfake technology, it is crucial to implement strong authentication mechanisms, especially in organizations that manage sensitive data or provide high-risk services. Neglecting this could leave them vulnerable to fraudulent actions and unauthorized transactions. Consequently, continuous research and the development of advanced detection methods are vital for protecting digital integrity. Furthermore, regulatory frameworks ought to be established to foster an inclusive environment that emphasizes safeguarding all stakeholders, including at-risk populations, thereby ensuring ethical and responsible AI utilization.

Authors Analysis

The author's analysis explores the intricate intersection of deepfake technology and its legal implications, particularly in relation to defamation and criminal liability, with an emphasis on the Bharatiya Nagrik Suraksha (BNS) Act. The paper emphasizes the obstacles encountered by Indian law in confronting deepfakes, due to the absence of specific legislation designed to address this emerging challenge. Although existing statutes, such as the Information Technology Act and the Indian Penal Code, tackle related offenses including privacy violations, identity theft, and defamation, they do not explicitly encompass deepfakes, thereby creating substantial gaps in enforcement and leaving victims with restricted options for recourse. The analysis highlights the challenges of applying conventional legal principles such as mens rea (guilty mind) and actus reus (guilty act) to AI-generated content, as deepfakes can be produced without human intervention, making it difficult to establish intent in defamation cases.¹⁷ The author stresses the necessity for the BNS Act to address these deficiencies by

¹⁷ Athulathmudali, Lalith W. "The Law of Defamation in Ceylon: A Study in the Inter-Action of English and Roman-Dutch Law." *The International and Comparative Law Quarterly*, vol. 13, no. 4, 1964, pp. 1368–406. JSTOR

integrating AI-related offenses, thereby ensuring enhanced protection for individuals against the misuse of technology.¹⁸ The paper recommends improved AI detection systems, more explicit legislation, and stronger enforcement mechanisms under the BNS Act to reduce the harm inflicted by deepfakes. Furthermore, it underscores the significance of ongoing technological advancements to identify and avert misuse, arguing for a comprehensive legal framework to protect digital integrity and human rights in the progressing digital environment.

Recommendation

The recommendation to tackle the challenges presented by deepfake technology, particularly in the context of defamation and criminal liability under the Bharatiya Nagrik Suraksha (BNS) Act, encompasses several essential measures.

First, the BNS Act ought to include specific provisions that criminalize the creation and distribution of deepfakes. This would address the existing legal void within current legislation, ensuring that individuals are safeguarded against digital defamation, identity theft, and privacy breaches that arise from AI-generated content. Explicit statutory language would assist in preventing misuse and guarantee accountability for those who create and disseminate deepfake content.

Second, the government must allocate resources to invest in and mandate the deployment of AI-driven detection tools designed for identifying deepfakes. Law enforcement agencies and the judiciary should be furnished with advanced technologies capable of detecting and analyzing manipulated digital content. Such measures would facilitate effective enforcement and aid in gathering accurate evidence in cases of defamation and other criminal acts associated with deepfakes.

Third, the BNS Act should provide a definition of how *mens rea* (guilty mind) and *actus reus* (guilty act) are applicable to offenses generated by AI. This clarification would ensure accountability for individuals who misuse AI technology for illegal objectives, even when the content is produced autonomously by AI systems.

Furthermore, it is imperative that policymakers, law enforcement, and legal professionals

¹⁸ *Id* Pg. 8, Note 10

receive training to comprehend the intricacies of AI technologies. This would enhance their capacity to effectively manage cases involving digital defamation and deepfakes.

Lastly, the importance of international collaboration and the harmonization of laws cannot be overstated. Considering the borderless nature of digital technologies, partnering with other nations to cultivate uniform legal frameworks will bolster the enforcement of laws against deepfakes and safeguard individuals worldwide from digital harm.

Conclusion

Deepfake technology, while providing certain advantages, presents considerable dangers to privacy, security, and public trust, particularly when it is misappropriated. India's current legal frameworks are insufficient to effectively tackle the threats posed by deepfakes, rendering individuals susceptible to defamation, cyberbullying, and misinformation.

The 2023 deepfake incident involving Rashmika Mandanna underscored the potential damage that such technology can inflict. In light of India's intricate socio-legal environment, there exists an urgent necessity for timely legislative measures to alleviate the risks associated with deepfakes. The country's growing acknowledgment of these threats, combined with the forthcoming implementation of the DPDP Act, offers a significant opportunity for India to establish targeted legislation to deter the misuse of deepfakes. This initiative will assist in safeguarding individual rights and preserving the moral and social framework of the nation.

References

- Information Technology Act, 2000
- Indian Penal Code, 1860
- Bharatiya Nyaya Sanhita, 2023
- The Protection Of Children From Sexual Offences Act, 2012
- Athulathmudali, Lalith W. "The Law of Defamation in Ceylon: A Study in the Inter-Action of English and Roman-Dutch Law." *The International and Comparative Law Quarterly*, vol. 13, no. 4, 1964, pp. 1368–406. *JSTOR*
- Olga Jurasz & Kim Barker, *Sexual Violence in the Digital Age: A Criminal Law Conundrum?*, 22 GERMAN L.J. 784 (August 2021).

- D. Nicholas Allen, *Deepfake Fight: AI-Powered Disinformation and Perfidy under the Geneva Conventions*, 3 NOTRE DAME J. ON EMERGING TECH. 1 (November 2022).
- Catharine A. MacKinnon, *Pornography as Defamation and Discrimination*, 71 B.U. L. REV. 793 (November 1991).
- Kingra, S., Aggarwal, N. and Kaur, N. (2022). Emergence Of Deep-fakes And Video Tampering Detection Approaches: A Survey. *Multimedia Tools and Applications*.
- Agarwal, A. (2024). *Deepfake-Related Rules In 7-10 Days: Govt. To Tech Firms*.

