https://doi.org/10.69974/mtzxrc12

GLS KALP
Journal of Multidisciplinary Studies
Volume 4; Issue 3;
July - September 2024

AI's Trojan Horse: The Deepfake Conundrum Under The Criminal Justice System

Sanjana Kothari[1]
Shaumya Tibrewala[2]

Abstract

This paper seeks to address an emerging challenge in the criminal justice system: the advent of deepfake technology. A concept which can be symbolised as AI's Trojan Horse – deepfakes, refers to highly realistic AI-generated audiovisual content – which have increasingly become indistinguishable from authentic recordings. Their existence poses unprecedented threats to the integrity of evidence, especially in the criminal law field, which serves as a watershed moment in the administration of justice. The paper's exploration will begin with a foundational understanding of deepfake technology, delineating its evolution and operational mechanisms. This background is vital, as it sets the stage for understanding the complex legal challenges deepfakes introduce, particularly in undermining the sanctity of evidence in criminal trials. By analysing the potential for deepfakes to compromise a defendant's right to a fair trial, the research will highlight a critical gap in current legal frameworks and evidentiary standards, calling for pressing legal reforms and technological safeguards. Further, the question of appointing a corporate personhood to artificial intelligence will be deliberated upon, touching upon the socio-legal implications of the same. The paper will conclude by reflecting upon the future trajectory of deepfakes and their impact on the legal landscape, affirming the need for ongoing vigilance and adaptation in judicial administration.

Keywords: *Deepfakes, AI, Evidence, Detection, Criminal Procedural Law*

Introduction

Deepfakes refer to synthetic media in which existing images or videos are manipulated using artificial intelligence (AI) techniques to create realistic, yet fake content[3]. The term "deepfake" was coined in 2017[4] and gained widespread attention due to its potential for misuse and manipulation. Deepfakes are created by using deep learning algorithms to analyze and manipulate large datasets of images and videos, allowing the AI system to generate highly convincing and often indistinguishable fake content.

The emergence of deepfake technology poses significant challenges and implications for the Indian legal system, particularly in the field of criminal justice. As we navigate this complex landscape, it becomes apparent that the implications extend beyond technological novelties, raising profound concerns about evidence integrity, identity theft, witness credibility, misinformation, and authentication hurdles.

---

[1] Law Student, BBA LL.B., Gujarat National Law University
[2] Law Student, BBA LL.B., Gujarat National Law University
[3] Alison Grace Johansen, *Deepfakes: What they are and why they're threatening,* NORTON, (January 26, 2024, 9:30 PM), https://in.norton.com/blog/emerging-threats/what-are-deepfakes.
[4] Meredith Somers, *Deepfakes, explained,* MIT (January 26, 2024, 9:50 PM), https://mitsloan.mit.edu/ideas-made-to-matter/deepfakes-explained.

One of the most pressing issues stemming from the proliferation of deepfakes is their potential to tamper with evidence[5]. In criminal cases, where the authenticity of evidence is pivotal in determining guilt or innocence, the capacity of deepfake technology to craft convincing yet false narratives pose a significant hurdle. Deepfakes also open the door to identity theft and impersonation[6], as they can seamlessly superimpose faces onto different bodies or alter voices. This introduces the risk of innocent individuals being falsely accused of crimes they did not commit, as malicious actors exploit the technology for nefarious purposes.

Further, the manipulation of witness testimonies through deepfake technology introduces another layer of complexity to courtroom proceedings. Fabricated videos featuring individuals providing false statements have the potential to undermine witness credibility and inject confusion into legal proceedings.

The detection and authentication of deepfakes present a formidable challenge for forensic experts and legal professionals alike. To ensure the reliability of digital evidence, it is imperative to develop robust methods for authentication that can keep pace with the evolving sophistication of deepfake technology.

Evidence in the Criminal Justice System

Technological advancements have been transforming various sectors, and criminal law system of India is no exception. The Indian Evidence Act of 1872[7] is the primary colonial era statute, enumerating rules governing evidence admissibility in Indian tribunals and courts. The 2023 winter session of the Indian Parliament witnessed the grant of presidential assent to three new criminal law bills which seek to replace the Indian Penal Code, Code of Criminal Procedure and the Indian Evidence Act, namely, the Bharatiya Nyaya Sanhita[8], Bharatiya Nagarik Suraksha Sanhita[9] and Bharatiya Sakshya[10] Acts of 2023. The paper shall delve into the key modifications proposed by the new evidence statute with regards to admissibility of electronic evidence, and how it could hypothetically play out in the day and age of deepfake technology.

Purpose of Study

The concern with the advent of artificial intelligence and technology is that it raises significant questions for the administration of justice in the Indian criminal system. How can courts determine the authenticity of evidence in the face of advanced deepfake technology? Will the credibility of witness testimonies be compromised? Can deepfakes be used to frame innocent individuals or to discredit legitimate evidence? Is there a possibility of appointing a corporate personhood to artificial intelligence? These questions highlight the urgent need for legal frameworks and regulations to address the potential misuse of deepfake technology.

---

[5] Chesney, Bobby and Danielle Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security,* 107 Calif. L. Rev. 1753, 1753-1820 (2019).

[6] Rene Hendrikse, *How Deepfakes Could Become A Threat To Your Identity*, FORBES, (January 29, 2024, 6:30 PM), https://www.forbes.com/sites/renehendrikse/2019/12/20/how-deepfakes-could-become-a-threat-to-your-identity/?sh=43ef3a010635.

[7] Indian Evidence Act, 1872, § 65, No. 1, Acts of Parliament, 1872 (India).

[8] Bharatiya Nyaya Sanhita (Second), 2023, No. 173, Bills of Parliament, 2023 (India).

[9] Bharatiya Nagarik Suraksha (Second) Sanhita, 2023, No. 174-C, Bills of Parliament, 2023 (India).

[10] Bharatiya Sakshya (Second), 2023, No. 175, Bills of Parliament, 2023 (India).

An Overview of Deepfake Technology

Technical Aspects

Deepfakes, a portmanteau of "deep learning" and "fake," refers to manipulated or synthesized media content created using artificial intelligence (AI) techniques, particularly deep learning algorithms[11].

The technical process of creating deepfakes commences with the collection of a large dataset of the target person's images or videos. Then, a deep learning algorithm, such as a Convolutional Neural Network (CNN), is trained on this dataset[12]. The algorithm learns the facial features and expressions of the target person to create a face model. Next, the algorithm is fed with the source media, which could be images or videos of another person, the source face. It analyzes the facial landmarks and expressions in the source media and maps them onto the face model of the target person[13]. To further enhance the realism of the deepfake, additional techniques like generative adversarial networks (GANs) can be used[14]. GANs consist of two neural networks, a generator and a discriminator, that work together to generate realistic media. The generator creates the deepfake images or videos, while the discriminator tries to distinguish between real and fake media[15]. This adversarial process helps improve the quality and authenticity of the deepfake. Once the deepfake is generated, it can be further refined by adjusting various parameters like lighting, background, and audio synchronization. The final result is a highly convincing video or image that appears to depict the target person in the commission of an act that never manifested in reality. Forensic techniques to detect generative AI are, safe to say, not the most advanced or accessible tools. A multifaceted approach is essential, involving substantial investment in resources and training, continuous research, development of standardized protocols and a commitment to ethical practices.

Impact of Deepfakes on the Right to Fair Trial

Deepfakes can be used to fabricate evidence, manipulate witness testimonies, or even impersonate defendants or key participants in a trial. Such manipulations can lead to wrongful convictions, undermine trust in the justice system, and jeopardize the fundamental principles of justice. A myriad of digital manipulation techniques, such as face swapping, voice synthesis, and intricate body movements, further compounds the challenge of ascertaining the authenticity of videos presented as evidence. Adding another layer of complexity, deepfake creators can manipulate metadata, including timestamps and geolocation data, to enhance the illusion of realism. This manipulation undermines the

---

[11] PUBLICATIONS OFFICE OF THE EUROPEAN UNION 2022, https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_Innovation_Lab_Facing_Reality_Law_Enforcement_And_The_Challenge_Of_Deepfakes.pdf (last visited Jan. 7, 2024).

[12] Aarti Karandikar, Vedita Deshpande, Sanjana Singh, Sayali Nagbhidkar, Saurabh Agrawal, *Deepfake Video Detection Using Convolutional Neural Network*, INTERNATIONAL JOURNAL OF ADVANCED TRENDS IN COMPUTER SCIENCE AND ENGINEERING (January 24, 2024, 8:30 PM), https://www.warse.org/IJATCSE/static/pdf/file/ijatcse62922020.pdf.

[13] Prof. Shashi Rekha G, Anusha D V, Muskan, Rakshith K Panchalingalu, Sahitya Modi, *Deepfake: Creation and Detection using Deep Learning*, IJRASET JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (January 22, 2024, 2:30 PM), https://www.ijraset.com/research-paper/deepfake-creation-and-detection-using-deep-learning.

[14] Olympia A. Paul, *Deepfakes Generated by Generative Adversarial Networks,* GEORGIA SOUTHERN UNIVERSITY (January 16, 2024, 8:30 PM), https://digitalcommons.georgiasouthern.edu/cgi/viewcontent.cgi?article=1742&context=honors-theses.

[15] *Ibid*.

reliance on metadata alone to establish the authenticity of evidence, necessitating a more nuanced approach to verification.

Beyond the technical intricacies lies the potential impact of deepfake evidence on the trial process and verdicts. The credibility of video evidence itself becomes susceptible to erosion if presented without robust authentication, casting doubts on the reliability of the evidence and potentially influencing trial outcomes. The insidious use of deepfakes to manipulate witness testimony introduces a new dimension of concern. Videos created to falsely implicate innocent individuals or manipulate the statements of witnesses inject confusion and doubt into the judicial process[16], creating a complex web for the judges to navigate.
As deepfake evidence becomes more prevalent, the prosecution faces an increased burden of proof. Establishing the authenticity or manipulation of a video may require additional evidence and expert testimony, adding layers of complexity to an already intricate legal process[17]. The consequences of deepfakes and evidence authentication ripple through the judicial system, potentially leading to delays in court proceedings. The need for expert testimony and the intricate nature of deepfake detection can prolong trials, impacting the overall efficiency and effectiveness of the judicial system.

Legal Discourse on Deepfakes

Statutory Recourses

Criminal Law

Since concerns regarding deepfakes are relatively new in the Indian legal landscape, there exists no statute presently which criminalises creation and use of deepfakes. Nonetheless, *vide* **Section 191** of the **Indian Penal Code 1860**[18], which criminalizes presenting false evidence, and **Section 192**[19], which penalizes fabricating false evidence, the use of deepfakes as a means to manipulate witness testimonies or fabricate evidence in a trial can be combatted.

Information Technology Law

Additionally, **Section 66D** of the **Information Technology Act of 2000**[20] (‘**IT Act**’) is concerned with identity theft, which could play out to be relevant when deepfakes are used to impersonate defendants or key participants in a trial. The provision imposes penalties for such offenses, ensuring that those involved in creating or using deepfakes for malicious purposes can be held accountable.

Further, as reiterated in *Myspace Inc v. Super Cassettes Industries Ltd.*[21], **Section 79**[22] of the **IT Act** demands that Indian intermediaries erase unlawful content upon receipt of actual knowledge or a court order.

Digital Personal Data Protection Law

[16] Yash Dahiya, *The Rise Of Deepfake Technology: A Threat To Evidence In Arbitration?,* LIVE LAW (January 12, 2024, 2:30 PM) https://www.livelaw.in/articles/the-rise-of-deepfake-technology-a-threat-to-evidence-in-arbitration-242718.
[17] Palmiotto Francesca, *Detecting Deep Fake Evidence with Artificial Intelligence: A Critical Look from a Criminal Law Perspective,* SSRN (January 25, 2024, 7:30 PM), https://ssrn.com/abstract=4384122.
[18] Indian Penal Code, 1860, § 191, No. 45, Acts of Parliament,1860 (India).
[19] Indian Penal Code, 1860, § 192, No. 45, Acts of Parliament,1860 (India).
[20] Information Technology Act, 2000, § 66D, No. 21, Acts of Parliament, 2000 (India).
[21] Myspace Inc. v. Super Cassettes Industries Ltd., (2017) 236 DLT 478.
[22] Information Technology Act, 2000, § 79, No. 21, Acts of Parliament, 2000 (India).

The **Digital Personal Data Protection Act of 2023**[23] (‘**DPDPA’**) establishes the role of data fiduciaries in safeguarding personal data from being exploited for different purposes, such as the likes of deepfakes. A Data Fiduciary is defined as any person who determines the techniques and intentions for which an individual's personal data will be utilized. A Data Principal is an individual whose data is collected by a Data Fiduciary. Personal data under the act is defined as any piece of information about a person that may be used to identify them. One's private images or videos shared online consequently fall under the criterion of personal data as per the **DPDPA**, which are subsequently utilized to build generative AI models that produce deepfakes. Data Fiduciaries should be compelled to implement extra protections to guarantee compliance with this responsibility. This may be achieved by prohibiting the download of personal media, or regulating how material data may be shared on a platform. **Section 8(6)**[24] of the **DPDPA** requires Data Fiduciaries to notify the Data Principal as soon as a breach is found. This will enable the Data Principal to take action even before such data is abused, by reporting it to the respective legal entities.

However, accounting for the fact that deepfake technology has not been statutorily recognised as of yet, it leaves a blaring lacuna in the law which the **DPDPA** is not able to undertake in its actual sense. The Act’s silence on generative AI is concerning, at the very least. Despite having made accommodations for a grievance redressal and appellate system, the incidence of deepfake encounters have not changed, if not increased. Recent escapades include Ukranian President Zelenskyy’s video asking his citizens to surrender to Russia, Indian sports personality Sachin Tendulkar’s video on endorsing an online gaming application, or actress Rashmika Mandanna’s deepfaked video. The intent with which the **DPDPA** was propagated, is not being met in implementation at the present moment, thereby having been termed as the ‘rubber stamp’ of data privacy authority.

The Ministry of Electronics and Information Technology (‘**MeitY**’), *vide* a press release dated July 2023[25], put out an advisory warning to social media platforms, alerting them to the potential consequences of allowing deepfake information to remain on their platforms[26]. The notification also proposed a regulatory framework that seeks to establish an independent statutory authority, alongside a Multi-Stakeholder Body (‘**MSB’**) for advisory purposes. It emphasized categorizing cases of usage of AI based on risk levels and regulating them under responsible AI principles. They also urged for the creation of the Artificial Intelligence and Data Authority of India (‘**AIDAI’**), which would ensure effective oversight and governance in the rapidly evolving domestic landscape of AI.

Drawing Global Parallels

In the international space for addressing artificial intelligence, the European Union is a pioneer in being the first region to adopt an AI Act. The **AI Act**[27] introduces a risk-based classification system, categorizing AI systems into various risk levels with stricter regulations for "high-risk" ones, including some deepfakes. This framework aims to balance

[23] Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
[24] Digital Personal Data Protection Act, 2023, § 8, No. 22, Acts of Parliament, 2023 (India).
[25] Ministry of Communications and Information Technology [Press Release No. 62/2023].
[26] Aihik Sur, *Tech Policy in 2023: From DPDP Act to net neutrality concerns, deepfakes, new telecom law and more*, *MONEYCONTROL* (February 13, 2024, 10:30 AM), https://www.moneycontrol.com/news/business/tech-policy-in-2023-from-dpdp-act-to-net-neutrality-concerns-deepfakes-new-telecom-law-and-more-11974371.html.
[27] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS (COM (2021)0206 – C9-0146/2021 – 2021/0106(COD)).

societal concerns with innovation. Transparency and explainability are emphasized, requiring developers to provide clear information about AI systems to foster trust and accountability[28]. Further, the significance of human oversight is highlighted, particularly for high-risk systems, with prohibitions on harmful applications like deepfakes used for social scoring or manipulating minors. These measures establish ethical boundaries for AI development, guarding against societal harm. While not directly relevant in India, this European statute provides a model framework for our legislative pillar.

Implications on the Admissibility of Criminal Evidence

Indian Evidence Act, 1872

The Indian Evidence Act of 1872[29] (**'IEA'**) provides the general guidelines for admissibility of evidence in court. Vide the amendment of 2000, it adjusted for evidence to include electronic records, as has been iterated under the Interpretation section, i.e., **Section 3**, as well as **Section 65A** and **65B**. As far as this Act is concerned, "*any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer (hereinafter referred to as the computer output) shall be deemed to be also a document*". This however, is subject to several conditions and safeguards laid down under **Section 65B (2)**, such as: person had lawful control over use of the said computer; the information so derived from it was a regular input in the ordinary course of activities; the computer had not been malfunctioning during the respective period; and lastly, a certificate that had to be issued purporting the validity and authenticity of the electronic record "*by a person occupying a responsible official position in relation to the operation of the relevant device*".

Bharatiya Sakshya Adhiniyam, 2023

The passing of the **Bharatiya Sakshya Act of 2023** (**'BSA'**) brings the criminal justice system to a watershed moment, owing to the fact that it brings about monumental changes with regards to widening the ambit of what constitutes evidence[30]. The Act recognizes the significance of digital evidence in modern-day crimes and the need to ensure its admissibility to promote fair and efficient justice delivery. Digital evidence refers to any information or data that is stored, transmitted, or processed in the digital form.

"*One is to accept electronic record on emails, server logs, documents on computers, laptop or smartphone, messages, websites, locational evidence and voice mail messages stored on digital devices as documents*", and thereby as admissible as evidence under **Section 2(e)(ii)**[31].

Further, **Section 57** of the **BSA** has been expanded to bring within its purview electronic and digital data as **primary evidence**. The statute has also gained strides in recognizing that digital or electronic records are legally equivalent to their traditional paper

[28] Ravi Singhania, Rudra Srivastava, Shambhu Sharan, *Navigating the Legal Landscape of AI Deepfakes in India,* SINGHANIA AND PARTNERS (February 27, 2024, 10:50 AM), https://singhania.in/blog/navigating-the-legal-landscape-of-ai-deepfakes-in-india.

[29] Indian Evidence Act, 1872, § 65B, No. 1, Acts of Parliament, 1872 (India).

[30] Vaibhav Chadha, *Discussing The Discrepancies And Errors In The Bharatiya Sakshya Bill, 2023*, LIVE LAW (January 12, 2024, 5:10 PM), https://livelaw-gnlu.refread.com/articles/discussing-the-discrepancies-and-errors-in-the-bharatiya-sakshya-bill-2023-236843?infinitescroll=1.

31 Amit Gupta & Harisankar Mahapatra, Electronic Evidence In The Bharatiya Sakshya Bill, 2023 – Regressive Or Progressive?, Live Law (January 12, 2024, 5:40 PM), https://livelaw-gnlu.refread.com/articles/electronic-evidence-bharatiya-sakshya-bill-2023-regressive-progressive-239126?infinitescroll=1.

equivalents[32]. This measure guarantees that electronic records be given the same legitimacy, enforceability, and legal weight as paper documents while simultaneously acknowledging the widespread use of digital information[33].

The below mentioned is an excerpt from **Section 57**, which provides clarity as to what electronic or digital record is qualified to be admitted as primary evidence in legal proceedings.

*"**Explanation 4**.—Where an electronic or digital record is created or stored, and such storage occurs simultaneously or sequentially in multiple files, each such file is primary evidence.*

***Explanation 5**.—Where an electronic or digital record is produced from proper custody, such electronic and digital record is primary evidence unless it is disputed.*

***Explanation 6**.—Where a video recording is simultaneously stored in electronic form and transmitted or broadcast or transferred to another, each of the stored recordings is primary evidence.*

***Explanation 7**.—Where an electronic or digital record is stored in multiple storage spaces in a computer resource, each such automated storage, including temporary files, is primary evidence."*

There is a blaring lacuna under the **BSA** which seeks to be pointed out, insofar as conditions or guidelines regarding admissibility of digital evidence are concerned. Despite the new statute having widened the scope of electronic evidence as compared to the **Indian Evidence Act 1872**, unlike **Section 65B**, no explicit guidelines have been provided to safeguard the authenticity and reliability of the evidence so presented. There exists a conspicuous avenue for exploitation, *vide* potential use of deepfakes and generative AI to manipulate the digital or electronic evidence. As has been reiterated previously, these technologies have the capacity to fabricate electronic/digital evidence, blurring the lines between truth and manipulation. Consequently, there is a pressing need for the **BSA** to incorporate robust mechanisms to authenticate digital evidence and safeguard against malicious tampering or manipulation, thereby upholding the integrity of the administration of justice. Without such safeguards, the potential for miscarriages of justice and erosion of trust in the judicial system looms large.

Corporate Personhood of AI

The concept of corporate personhood, which grants legal recognition to corporations as entities separate from their owners, raises intriguing questions when applied to Artificial Intelligence (AI). Considering the autonomous nature of AI entities and their ability to act independently, there is a growing debate on whether AI should be granted a form of corporate personhood. This would entail treating AI as a legal entity capable of owning property, entering contracts, and potentially being held liable for criminal offenses.

Key considerations include establishing the physical i.e., *actus reus* and mental i.e., *mens rea* elements of criminal liability for AI entities, as well as determining appropriate punishments. *Actus reus* refers to the physical act or conduct that constitutes a crime, while

32 Chhtrapati, D., Chaudhari, S. P., Mevada, D., Bhatt, A., & Trivedi, D. (2021). Research Productivity and Network Visualization on Digital Evidence: A Bibliometric Study. Science & Technology Libraries, 1–15. https://doi.org/10.1080/0194262x.2021.1948486

33 Yuvraj P. Narvankar, Electronic Evidence Under The Bhartiya Sakshya Bill, 2023: A Pandora's Box To Be Reopened!!, Live Law (January 19, 2024, 11:30 AM), https://livelaw-gnlu.refread.com/articles/electronic-evidence-under-the-bhartiya-sakshya-bill-235353.

mens rea pertains to the mental state or intent behind the act. For AI entities, attributing these elements involves understanding the actions taken by the AI system and the intent or knowledge behind those actions.

Analogies may be drawn between AI entities and human offenders to provide a framework for assessing the appropriate level of accountability and punishment[34]. Comparing actions like permanent deletion of AI software to the death penalty suggests a severe consequence for AI entities that commit serious offenses or cause significant harm. This analogy implies that such actions could result in the complete cessation of the AI entity's functionality, akin to the irreversible nature of the death penalty for humans.

Similarly, equating temporary deletion of AI software to imprisonment draws a parallel between the temporary incapacitation of the AI system and the confinement of human convicts. This comparison reflects the idea of imposing a form of punishment that restricts the AI entity's capabilities for a specific duration, mirroring the concept of imprisonment in human criminal justice systems. These analogies help conceptualize the potential consequences and punishments for AI entities based on the severity of their actions and the harm caused.

However, implementing this concept raises complex challenges, such as defining the boundaries of AI's autonomy and decision-making capabilities, determining the extent of AI's legal rights and responsibilities, and establishing mechanisms for enforcing accountability[35]. While granting corporate personhood to AI could enhance clarity in assigning liability and promoting ethical behaviour, it also raises ethical and practical concerns. Questions regarding AI's capacity for intent, moral agency, and the potential consequences of holding AI criminally liable need careful consideration.

Recommendations

In response to the challenges posed by deepfake technology in legal arenas, the authors of this paper offer key recommendations. One approach is to enhance the awareness and education of judges, lawyers, and jurors about the existence and potential impact of deepfakes. This can enable them to identify and scrutinize potential manipulated evidence more effectively. Technological solutions can also play a crucial role in combating deepfakes. Developing advanced detection algorithms or forensic tools specifically designed to identify deepfakes could help expose manipulated evidence and ensure its exclusion from legal proceedings. Collaboration between technology experts and legal professionals can be fostered to develop effective countermeasures against deepfakes.

Additionally, legislatures can enact laws that explicitly criminalize the creation, distribution, or use of deepfakes for malicious purposes within the context of legal proceedings. Courts shall take a proactive stance in establishing guidelines or admissibility standards for digital evidence. These standards could require the authentication of digital evidence by expert witnesses or the submission of metadata and other technical information to verify its origin and integrity.

However, the first step towards initiating this course of action is to **call upon the legislative to recognise, by way of definition and interpretation, the term**

34 Ankit Kumar Padhy, Amit Kumar Padhy, Criminal Liability of the Artifical Intelligence Entities, 8 Nirma University Law Journal 16, 16-20 (2019).

35 Trivedi, D., Bhatt, A., Trivedi, M., & Patel, P. V. (2021). Assessment of e-service quality performance of university libraries. Digital Library Perspectives, ahead-of-print(ahead-of-print). https://doi.org/10.1108/dlp-07-2020-0072

'deepfake' technology under the criminal laws of India. Once due acknowledgement has been provided for, only then will the remedy be concrete.

Conclusion

The **Bharatiya Sakshya Adhiniyam of 2023**, as it currently stands, lacks specific provisions for the detection of deepfakes and guidance on judicial conduct regarding such evidence. This oversight signifies a crucial area for governmental action and legal reforms. The study, acknowledging various existing techniques for deepfake detection, underscores the profound implications of this technology for the Indian criminal justice system. It calls for the urgent integration of ethical AI practices and legal reforms to mitigate the risks associated with deepfakes. The Act's acknowledgment and widening of scope for electronic/digital evidence is a progressive step, yet, forensics continue to face hurdles due to the evolving complexity of deepfakes. This situation necessitates legal reforms, including criminalization of deepfake misuse and establishing reasonable guidelines for digital evidence admissibility. The study concludes by underscoring the need to enhance legal education, foster technological collaboration, and raise public awareness, thereby fortifying the legal system against the challenges posed by deepfakes.