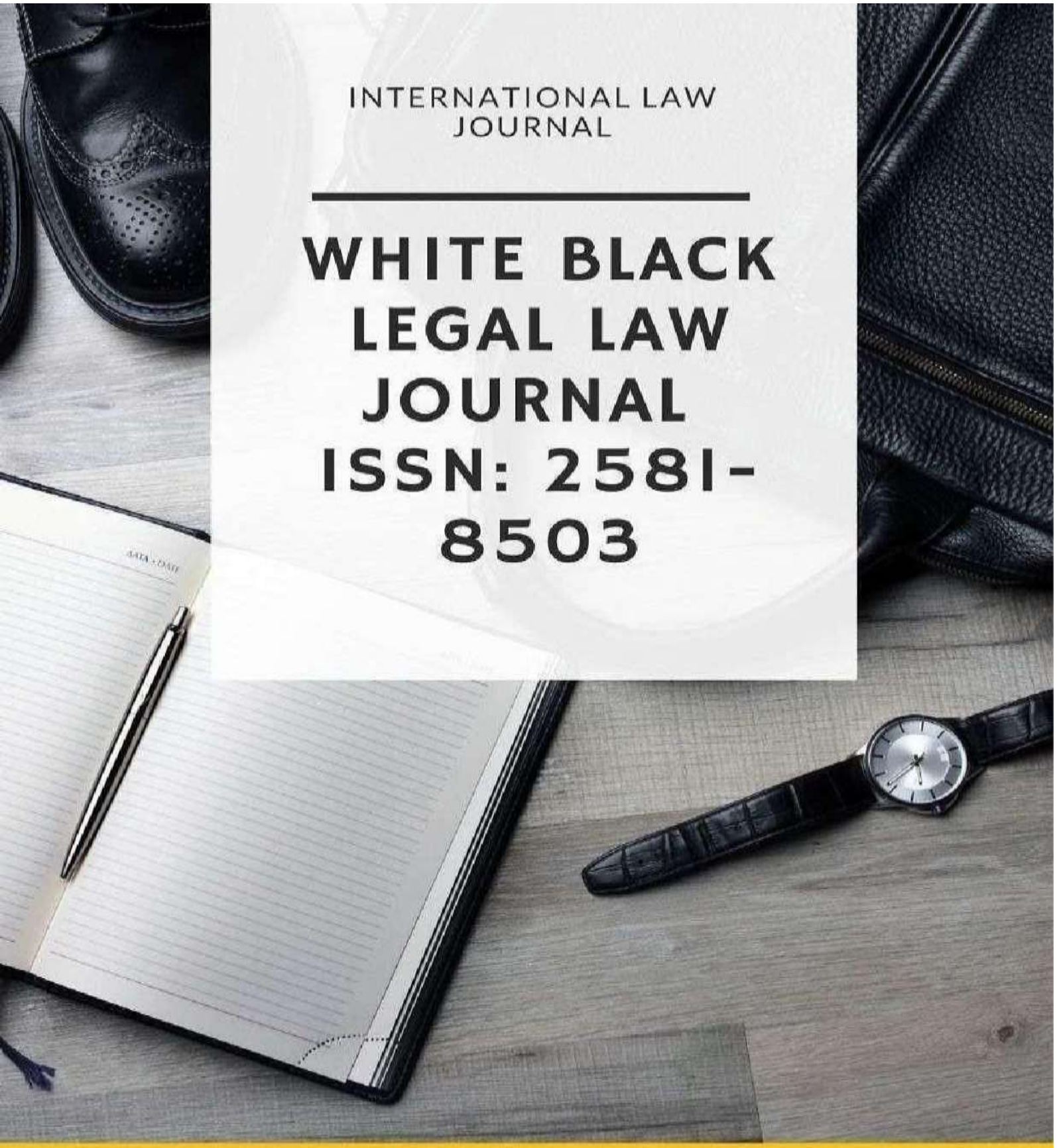

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

DISCLAIMER

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

DEEPFAKES AND THE CRISIS OF DIGITAL EVIDENCE: REFORMING INDIA'S EVIDENTIARY FRAMEWORK UNDER THE BHARATIYA SAKSHYA ADHINIYAM, 2023.

AUTHORED BY - SHRIHARI R
School of Law, CHRIST (Deemed to be University), Pune, Lavasa.

Abstract

Artificial Intelligence is evolving quickly, creating an environment that allows for deepfakes. Deepfakes are highly realistic fakes of audiovisual media. They create audio-visual evidence that's nearly indistinguishable from reality. Creating deepfakes poses a significant challenge to the legal system in India where courts are becoming increasingly reliant on digital evidence. The key issue is that the Bharatiya Sakshya Adhiniyam 2023 (BSA) has modernized evidence law in India. However, the BSA still focuses on procedural authentication through certification methods to authenticate evidence rather than focusing on substantive authentication. This paper will discuss how deepfake technology is creating an evidentiary crisis by degrading the reliability, integrity and admissibility of digital evidence creating a new phenomenon known as a "liar's dividend". Through doctrinal analysis, case law study, and comparative analysis from jurisdictions such as the European Union, United States and China, this paper will identify critical gaps in India's evidentiary framework. The paper's recommendations include moving to forensic-based authentication of digital evidence, developing mandatory protocols for detection of deepfakes, development of an institutional capacity for detection of deepfakes, and statutory reform. This study concludes that unless a technological safeguard is integrated into India's evidentiary framework, the accuracy of the Indian judicial system will be undermined leading to a loss of public confidence in the judicial system.

1. Introduction

Modernizing our legal system is greatly affected by digitizing the nature and use of evidence. More courts are using digital data, including CCTV, email, social media and electronic communications when making decisions about disputes. But, this shift is being driven by the introduction of new technologies to create deepfakes. Deepfakes are made using complex machine learning techniques like Generative Adversarial Networks (GANs) to produce hyper-realistic visual and audio media that can deceive others into believing a person did something

they actually did not do.

Deepfakes cause a fundamental change in the way we treat audiovisual evidence. We assume that we can trust such evidence because we can see it and therefore must believe it. That assumption is disrupted with the use of deepfakes because a very good and authentic video recording can be entirely created or duplicated using this technology. This places courts in a new era of epistemic uncertainty when trying to find the truth about facts as they were created. The issue of using deepfakes as evidence is even more difficult for courts in India than in many other countries and will become even more problematic with the Bharatiya Sakshya Adhiniyam, 2023 which is an attempt to modernise evidentiary rules and allow digital records to be treated as original evidence. The legislation still primarily places a procedural focus on the authentication of the digital record rather than placing a technological focus on verifying the authenticity of the record.

2. The Rise of Digital Evidence in India

The evolution of the evidentiary system in India has been a complicated and extensive process - at the beginning (colonial times), there was a very rigid understanding and application of the law surrounding the concept of evidence. Evidence was understood as having an oral component whereby Verbal Testimony from a Human was crucial in the application of the evidentiary law as well as having a physical component (actual documents). This was based on the limitations of the available technologies in the 19th century. Based on this premise, all of the applicable provisions of the evidentiary law were premised upon the existence of physical documentary evidence and the ability to prove authenticity based on testimonial evidence provided by a human. In early applications of the evidentiary doctrine, primary evidence consisted of original documents and secondary evidence as copies were treated with caution and therefore, very strict foundational proof was required in order to use the secondary evidence.

During the late 20th and early 21st century there was (more than ever) a proliferation of technology changes that made the evidentiary law framework increasingly obsolete, since the technological advancements of computers, advances in telecommunications, and the introduction of completely different storage options for electronic data presented an entirely new way of how data/information was created, transmitted, and preserved. Accordingly, the law making body (legislature) passed the Information Technology Act of 2000 that added sections 65a and 65b to the Indian Evidence Act of 1872, thus creating a watershed moment in

Indian evidence law as it contained provisions for the inclusion of electronic evidence in the evidentiary regime.

The sections 65A & 65b have created a new kind of framework for making electronic evidence admissible. So, they now have a separate way of doing things compared to how it used to be done with documents (This is called the “rules of documentary evidence”). Section 65A was an enabling section and allowed you to use electronic records as evidence. Whereas section 65b was detailed about how you could make electronic records admissible.

This new legislation is considered the next stage in the evolution of the law regarding the use of evidence in courts. The purpose of this law is to modernize and rationalize how courts treat types of evidence. The new law explicitly states that electronic records are "documents," which makes them primary evidence. The recognition of electronic records as primary evidence marks a significant change in how courts view electronic records because courts will no longer treat them as secondary or derivative forms of evidence, meaning that courts will recognize them as independent and reliable sources of evidence. The new law will also clarify admissibility rules; reduce ambiguities regarding certifying documents; and bring the law governing evidence into line with technological developments that have occurred since the prior law was passed.

Digital evidence is becoming increasingly important in litigation in India. Courts use all kinds of electronic evidence to help them decide a case; this includes video recorded from surveillance cameras, phone recordings, call details from phones, GPS data from travel and movement, emails, and communications on social media. The majority of times, this type of evidence will be critical in proving a timeline of events in criminal cases; supporting or contradicting witness testimony presented during trial; and connecting an accused person to a crime. Likewise, digital communications usually play a critical role in proving the existence of a contract between two parties, their intentions towards one another, and their actions towards one another. One of the reasons why there have been so many more instances of digital evidence being used is not just due to the enormous growth of digital media but also the willingness of judges within the judicial system in India to consider electronically stored information.

3. Deepfakes and the Crisis of Authenticity

Deepfake technology represents a two-fold and seriously disruptive challenge to judicial systems, affecting not only how evidence is created but also how it is evaluated. The ability to create seemingly “real” video or audio representations (e.g., an individual committing an act,

making an incriminating statement, or participating in a conspiracy) raises serious questions regarding the authenticity of all audiovisual evidence. Audiovisual evidence is often considered very powerful corroborating evidence in a court of law and can have a substantial impact upon investigators, prosecutors, judges, and even jurors. Consequently, it has the potential to cause many wrongful allegations and miscarriages of justice through the use of deepfake technologies.

The second aspect of this threat is more subtle and has more sinister ramifications than the first: the rise of the "liar's dividend." The strategic manipulation of deepfake technology can result in a party's being able to challenge the authenticity of legitimate evidence through an explanation of how synthetic media can create reasonable doubt when made public. In a case where a person is accused of wrongdoing, they may assert that legitimate audio or video evidence of their actions was created using computer-generated imagery, which would have otherwise not created reasonable doubt.

This has the effect of eroding the evidentiary value of legitimate digital records and undermining the ability of the law to hold a person accountable for their actions. While deepfakes add a level of false evidence to the evidentiary process, they also add a level of doubt to the truth as it relates to evaluating the integrity of the evidence in ways not previously experienced.

These two dynamics create what is being referred to as a crisis of authenticity. Traditionally, the common law evidentiary system, including that of India, is predicated upon the suspension of the assessment of credibility and probative value of evidence until the trial stage when the evidence is first admissible before the fact-finder, at which point, the fact-finder will determine whether the evidence is admissible based on whether it meets established parameters (e.g., evidence is relevant and has been authenticated) before entering the trial process to consider and assess the credibility and probative value of evidence through competing narratives and cross-examination.

The evidentiary model presupposes that there is sufficient evidence of authenticity established at the threshold to enable the fact-finder to assess actual credibility of the evidence and determine actual significance (e.g., weight) at the trial. This structure for establishing credibility of evidence is fragmented by deep fakes creating the resolution between admissibility and weight impossible. When there is question as to the credibility of evidence itself, courts will now be confronted with complicated technical issues, even before the laws of admissibility are established. There are so many more issues than just relevance and source when it comes to admissibility; essentially the question becomes; is it real? This presents a

paradox for courts in evidence determination. If the court admits evidence, that may be fabricated, they run the risk of tainting the fact-finding process. On the other hand, if courts refuse entrance of evidence that may be manipulated, they may exclude evidence that is actually real. This presents a significantly greater amount of uncertainty about how evidence can be presented than what presently exists through evidentiary law.

This uncertainty is particularly apparent within the framework of Indian evidence law as it pertains to digital evidence due to the reliance upon digital evidence in the majority of current litigation/ criminal prosecutions. Digital evidence is now the most widely accepted form of evidence within civil and criminal cases and is being utilised as primary and supplementary forms of evidence within the majority of criminal prosecutions and civil disputes. Examples of digital evidence routinely relied upon to establish presence and involvement at a crime scene include CCTV footage, call data records, and social media usage; the advent of deepfake technology creates multiple opportunities for the misuse of digital evidence.

Misleading videos could be created in many ways to create false alibis or frame enemies. Fake audio could be made to assist in extortion, fraud, and defamation. Also, synthetic media could be used for malicious purposes, including misleading voters during political campaigns or damaging the credibility of others, especially well-known figures.

These implications affect not only single cases, but they also affect the overall integrity (trustworthiness) of the entire legal system. The functioning of the justice system relies heavily on the ability of courts to establish facts as true with a high level of accuracy. When an item of proof is in doubt due to the possibility of it being modified (either by technical means or by someone else), there is an increase in the likelihood of a wrongful determination being made. It is also likely that when there is a strategic usage of deepfakes, litigation will also be altered. Even reliable proof will be challenged if it can be shown that a deepfake was used, thereby potentially extending the timeline for a case to be resolved and imposing additional costs to the court system due to having technical disputes to be resolved during the time of litigation, which were previously insignificant to the court process.

4. Legal Framework under the Bharatiya Sakshya Adhiniyam, 2023

With the passing of the Bharatiya Sakshya Adhiniyam, 2023, India has made a great leap toward modernizing its evidentiary framework as it has recognized the importance of digital evidence in legal proceedings. By recognizing 'electronic records' as the primary type of evidence and streamlining admissibility standards, the new law attempts to bring evidentiary

law up to date with the current state of technology. Although the new law has provided some improvements over the previous evidentiary law, it does have serious limitations in dealing with the challenges posed by new forms of deepfake technology.

The current evidentiary framework continues to rely heavily on established procedural safeguards intended to protect against tampering of electronic evidence. These safeguards include certifying the electronic evidence; properly documenting the chain of custody; providing evidence to verify that the metadata of the electronic evidence is accurate; and, when necessary, providing expert testimony. Collectively, those objectives are intended to prove that the electronic evidence has been collected from a reliable source, properly secured, and has not been tampered with during transport or stored in a manner that would raise a reasonable doubt as to its authenticity.

5. Comparative Jurisprudence

An analysis of the response of the Global Community demonstrates that some jurisdictions are taking proactive steps to meet evidentiary and regulatory challenges posed by deepfake technology. While these jurisdictions have developed unique approaches with varying scope and intensity, there appears to be a common trend whereby jurisdictions recognize that traditional evidentiary doctrines, developed in the analog or early digital era, are insufficient to deal with AI generated synthetic media. To that end, jurisdictions appear to be developing entities and frameworks that emphasize transparency, traceability and the integration of technology.

In the European Union, regulatory measures are being developed based on a risk based approach to artificial intelligence. Under the evolving AI regulatory framework, deepfakes are characterized as high-risk or sensitive due to their potential to mislead or cause harm. Thus, regulatory emphasis is on transparency, with synthetic media businesses being subject to clear disclosure obligations indicating that synthetic media has been artificially generated or artificially manipulated. This includes labelling requirements and, in some circumstances, requiring technical markers to automatically signal that synthetic media contain synthetic content. The goal is not just to punish misuse after the fact, but to provide users, regulators and adjudicators with tools to identify synthetic content when interacting with such content.

In the U.S., the laws respond to deepfakes differently but are nevertheless very important. States have made new laws addressing the use of deepfake technology in certain areas, such as political campaigns and elections. These laws require that the use of synthetic/virtual media in

campaign or political ads be disclosed so that voters know they are not being manipulated and that the democratic process is being preserved. At the national level, policymakers have begun to shift their focus toward the need for broader accountability measures for AI-generated evidence, especially in litigation. While there is still work to be done on developing a comprehensive set of federal regulations, people in courts and Congress are beginning to recognize that the standards of admissible evidence must change in order to deal with the risks of the false creation of digital content. Additionally, courts in the U.S. have shown a willingness to consider expert testimony and supporting evidence (forensic analysis) when dealing with cases involving digital content manipulation which is indicative of a trend towards more technology-oriented decision making in litigation.

China has taken a much more centralized and stringent regulatory approach to deepfakes. The regulatory architecture of China emphasizes strict control of the creation and distribution of synthetic/virtual media. The regulations specifically prohibit the distribution of unlabeled deepfakes and put specific affirmative obligations on the service providers that allow consumers to easily identify synthetic media. China has mandated tracing digital media to keep track of where they originated and how they have been changed, in addition to using digital watermarks to assist with this process. China is also implementing new forms of verification after digital watermarks through blockchain technology to ensure that there will be a verifiable chain of authentic evidence that regulators, judges, and law enforcement can rely on. By incorporating technological safeguards into every phase of the digital content creation process, this new model will reduce evidence-related ambiguity right at the source.

Therefore, there are no specific regulations governing the treatment of deepfake evidence, which puts India's evidential framework substantially behind international best practice and leaves courts to rely on general authentication principles and expert evidence without a governance framework or technological assistance. Moreover, as deepfakes become more prominent, this gap will continue to increase, and will lead to judicial decisions being inconsistent and there will be confusion surrounding evidentially capable deepfakes.

Comparative jurisprudence emphasizes that India should adopt a more holistic strategy to incorporating legal systems with technology and institutions than just relying on a procedural method of confirming authenticity. To create a more robust evidentiary structure, India will need to utilize global best practices but modify them for Indian legal and constitutional settings in order to be able to resolve issues caused by synthetic types of media in the digital world.

6. Gaps in the Indian Evidentiary Framework

The foregoing analysis highlights that, despite significant legislative progress, India's evidentiary regime remains inadequately equipped to respond to the challenges posed by deepfake technology. These shortcomings are not isolated but structural in nature, reflecting deeper doctrinal, institutional, and technological limitations. The most critical gaps are outlined below.

6.1 Procedural Bias

The current framework has a significant flaw in that the emphasis placed on process-related requirements is too demanding. Specifically, the requirement for certification, for chain of custody, and for all technical documentation needed to prove that a record is admissible in court places the burden on the process of how electronic records are created and preserved rather than on the accurate content of what those electronic records contain.

In the case of deepfakes, the process-based bias creates issues for courts because the latter is an artificial creation and therefore does not have any basis in the real world (which is how the records are typically viewed). Because of this, a piece of synthetic media can meet every statutory requirement (e.g., it was created on a specific device, has the required certifications, and has been preserved without modification) and still be considered to be false.

The focus of the legal framework is on how evidence has been handled instead of what it represents; therefore, the framework fails to sufficiently address the risk of deepfake evidence. As a result, there is an inherent tension between the authenticity established by the process-based certification of electronic records and the truthfulness of the content of those records, thereby negatively impacting the reliability with which an evidentiary assessment can be made.

6.2 Absence of Forensic Standards

The absence of standardized forensic protocols to detect and evaluate deepfake content is another critical gap in the area of deepfake litigation. Currently, there are no mandatory guidelines for courts to use when determining whether suspected synthetic media is authentic. Without standard methodologies for the forensic analysis of suspected synthetic media, when forensic analysis is conducted, it typically occurs on a case-by-case basis and is dependent on the level of expertise and resources allocated to that particular case.

This lack of standardization has resulted in a great deal of inconsistency in how courts operate. Each court determines its own threshold for admissibility, consults with different experts, and

uses differing criteria to evaluate similar evidence but will not have the same standard benchmarks for accuracy, reliability, and validation of detection tools to assess the evidentiary weight of the forensic finding. Given the high degree of complexity of technology involved in determining whether media is authentic and the severity of the potential consequences, the lack of consistency and predictability in how the courts operate creates a major hurdle for the legal system as a whole.

6.3 Institutional Deficiency

A strong evidentiary framework will depend greatly on the ability of the courts to function; otherwise, they may lack significant capacity to carry out their functions. In many ways, India meets all of these challenges. Most courts do not have sufficient access to highly specialized digital forensic laboratories; or do not have sufficient access to the necessary tools to detect AI-generated evidence; and they do not have sufficient staff trained in analyzing AI-generated evidence.

Most judges and other legal practitioners lack sufficient technical literacy to critique highly technical and complicated forensic reports, and therefore rely on the opinion of others. These opinions may differ, and may not have been subject to any standard of evaluation. Lastly, delays in obtaining forensic analyses, and limited resources to obtain these analyses, can lead to lengthy delays in adjudicating cases. There is currently no dedicated institutional framework to handle deepfake evidence; thus, practical evidentiary safeguards cannot be effectively enforced.

6.4 Legal Vacuum

The lack of an explicit legal definition and a framework for proof of deepfake evidentiary use further contributes to the escalating gap in legal clarification. Although there are existing legal principles in terms of related injuries (i.e., fraud, impersonating someone, and cyber-related offenses) that can apply to AI-generated synthetic media, they do not contain an explicit definition of deepfakes or guidance on admissibility.

The absence of legislative clarification creates ambiguity for both courts and judges. Judges have no definitive authority upon which to base whether deepfake evidence is subject to a more stringent scrutiny of whether special rules of admissibility should prevail, or the allocation of the burden of proof in cases that involve the alteration of the authenticity of the deepfake. Therefore, judges are interpreting existing provisions in ways that do not fully support the technological implications of deepfakes in terms of the production and distribution of artificial

intelligence-generated media. As a result, there may be inconsistent legal findings regarding deepfakes and uncertainty over legal principles as litigation involving synthetic media substances continues.

6.5 Epistemic Uncertainty

The emergence of epistemic uncertainty with respect to the evidentiary process may be, perhaps, the most significant gap. The proliferation of deepfakes and the "liar's dividend" have resulted in a decline in the reliability of digital evidence as an accurate representation of truth. Therefore, parties to litigation will increasingly question the authenticity of evidence, regardless of its real reliability, and impact the ability to collect facts.

This decline in trust has implications that extend beyond the legal strategy and judicial outcome. For instance, prosecutors may experience difficulty in relying upon digital evidence to establish conviction, while defendants may use the potential of evidence manipulation as a way of casting doubt. Furthermore, in civil litigation, parties may contest the authenticity of email messages or other recorded communications that would have previously been accepted as conclusive evidence. The additional uncertainty will lead to a greater risk of wrongful convictions or unjust acquittals and will also increase the burden placed on courts to resolve complex technology-related disputes.

7. Reform Proposals

To tackle the issues caused by deepfakes, a comprehensive reform process is necessary. Deepfake technology requires more than simple modifications to current rules; a multi-faceted reform strategy is needed, one that utilises inventive doctrines, advances in technology and the strengthening of institutions. In light of this, the proposals below will help to reconfigure India's evidence law in a way that allows the courts to fulfil their truth-seeking role within the increasingly complex environment of digital information.

7.1 Substantive Authentication Standards

The first step to reforming evidence law is for practitioners and the courts to begin to distinguish between two different types of authentication: (1) procedural or technical/authentication (2) substantive authentication, where procedural or technical/authentication by itself is not adequate for determining substantive authenticity. Current admissibility rules treat procedural or technical/authentication (that is, origin and

integrity) as the only form of authentication and therefore admissibility criteria. As such, current evidentiary rules are confined to verifying the origin and integrity of the electronic record; they do not contain an explicit inquiry pertaining to substantive authenticity or genuineness.

For example, court rules should require that the court determine whether audiovisual evidence accurately reflects real events, i.e., if there has been any alteration or manipulation of the material. To accomplish this, the courts need to develop specific doctrinal standards and factors to assess audiovisual evidence on substantive grounds in addition to procedural or technical authentication. Some suggested examples of these types of standards or factors include: contextual consistency, corroborative evidence, and forensic validation.

By incorporating substantive authenticity (genuineness) into admissibility thresholds for evidence, all parties will be better protected from the admissibility and use of convincingly fabricated evidence.

7.2 Mandatory Forensic Verification

Due to the complexity of deepfakes, traditional evaluation methods alone are inadequate to assess their authenticity. Forensic examination of any digital evidence (both visual and/or audio) should be mandated by the courts if there is a dispute regarding the evidence, or if there are valid reasons to doubt it. Forensic examinations can include both traditional forensic techniques such as the analysis of metadata and verification of devices, as well as more sophisticated detection tools, including artificial intelligence based systems that can identify anomalies in visual and audio data.

7.3 Institutional Capacity Building

In addition to having the appropriate laws in place, there needs to be an institutional readiness for the implementation of legal reform. Part of this institutional readiness requires the establishment of specialized digital forensic labs which will utilize cutting-edge technology to assist courts in assessing complex forms of electronic evidence. These specialized institutions should be established at both the centre and state levels to provide access to all parts of the jurisdiction.

Human capacity development is equally important, as those involved in the judicial process – judges, prosecutors, defense lawyers and investigators – need to be trained in the basic principles of digital evidence, AI and forensic analysis. Ongoing judicial education programmes can increase the technology knowledge level of judges, so that they can better

evaluate the credibility of their expert witnesses, and have a better understanding and engagement with the technical aspects of digital evidence. If the requisite capacity-building measures are not put in place, then even the best legal standards are likely to fail in practice.

7.4 Statutory Recognition of Deepfakes

The need for a clear and definitive statutory framework for addressing deepfakes is due to the ambiguous nature of the existing law, as well as the lack of doctrinal clarity regarding how to evaluate or use this type of evidence. Legislation should provide definitions of deepfakes and other types of synthetic media that are generated using AI technology, differentiating them from traditional forms of digital evidence. Additionally, legislation should lay out the rules for how deepfake evidence can be admitted into court, including higher standards for proving that such evidence is authentic, as well as rules requiring the disclosure of any synthetic media in a case.

The establishment of such a framework would allow the law to more directly address the risks associated with deepfakes, rather than relying on indirect or analogous uses of current laws. It could also facilitate the creation of rebuttable presumptions concerning deepfake evidence, such as requiring additional proof of authenticity when the evidence at issue appears to be synthetic.

7.5 Technological Integration

The use of technology will become more prevalent in evidentiary practices as different forms of legal framework develop. Digital watermarking, cryptographic hashing, and blockchain-powered provenance tracking can help create a verifiable record of where a digital file came from or how it has been altered. By using these technologies within the life cycle of a digital file, we can greatly improve our ability to trace those files and reduce the opportunity for an undetected attack on them.

7.6 Burden-Shifting Framework

Due to the imbalance in available information and the difficulty to identify sophisticated deepfakes, it is appropriate to review how the burden of proving authenticity was assigned in some circumstances. Specifically, when credible allegations of tampering have been raised against a piece of evidence, then the party relying on that evidence may bear the burden of establishing authenticity, at least partially. Thus, this would create an incentive for the parties collecting and presenting electronic evidence to do so with greater care and for other parties to

rely on less doubtful evidence.

Such a framework will need to be designed carefully so that it does not violate fundamental principles of fairness, especially in relation to criminal cases. That said, when uniquely controlled by one party, the implementation of a carefully designed and calibrated mechanism to shift the burden of proof can create greater accountability and greater reliability of evidence.

8. Conclusion

Deepfake technology is fundamentally changing what we think about digital evidence and is forcing us to rethink some of our long-held beliefs about how we use evidence to prove or disprove things. The use of this technology allows for the creation of very realistic and convincing audiovisual materials that do not reflect reality, thus negating the very foundation of the belief that the audiovisual nature of evidence can be relied upon as a true representation of reality. While the Bharatiya Sakshya Adhiniyam, 2023 does a good job of recognizing electronic records and making strides towards modernization of procedure, it does so on a framework that is largely focused on formal compliance rather than true substantive evidence. This paper has shown that the current focus on certification, chain of custody, and processes that ensure procedural integrity are ineffective at dealing with the added complexity of AI manipulated evidence. Through deepfake technology, we see a gap between the appearance of authenticity and the actuality of fabrication, creating opportunities for manipulation or exploitation of this material throughout the judicial system. The comparative analysis demonstrates that while other jurisdictions have begun to address these challenges, they have done so by way of proactive regulation, integration of technology, and the development of clearer guidelines regarding standards for evidence.