ARTIFICIAL INTELLIGENCE: CRIMES AND EVIDENCE TAMPERING

ABSTRACT

In light of recent advances in technology and artificial intelligence, there have been a lot of efforts to integrate it into various fields including law. Evidence plays a very significant role in delivering justice, the reason being that a judge’s interpretation depends heavily on the evidence provided to them, and any meddling with the evidence can cause judge’ to lose their sight which becomes a hindrance in delivering justice duly and proficiently. In the eyes of the law, particularly in India, tampering with evidence is a serious offense under section 238 of Bharatiya Nyaya Sanhita. With the coming of Artificial Intelligence [AI] and its easy accessibility to everyone, tampering proof has become an effortless crime. This paper shall explore the rising concerns and the potential risks of evidence tempering in the AI age while emphasizing the indispensable link between technology accessibility and legal integrity. The paper also deliberates upon different types of tampering of evidence and how AI contributes or can potentially contribute to it. The paper shall also provide legal framework regulatory the admissibility of digital evidence and its effectiveness. The implications of these findings are profound, indicating a critical need for developing advanced forensic tools that can detect AI-generated tampering. This paper's conclusion will emphasize the necessity of technological and legal safeguards, including the advancement of cutting-edge forensic technology and the fortification of the legislative framework.

Keywords: *Artificial Intelligence, Evidence tampering, Forensic technology, AI crimes, Digital evidence*

INTRODUCTION

In an era marked by rapid digitization, it is platitudinous to say that Artificial Intelligence is indeed already reshaping and transforming many aspects of our real society and redefining the way we interact with technology. Along with several other industries, the justice system, too, stands at the steep cliff of a profound shift as AI integrates into every aspect of evidentiary process which includes evidence collection and its review which is presented before court of law in criminal trials to bring upon criminal justice to the victims. While this integration of AI into criminal proceedings offers unprecedented opportunities such as enhancing accuracy and efficiency in criminal investigations, plays the crucial role in recovering the lost evidence from accident and crime scenes which was recently being highlighted by Pune police who were utilising AI-based tools for the ‘digital reconstruction” of a Porsche car crash allegedly involving a juvenile driver.[1] NSAIL researchers have been in the forefront of developing systems to make realistic deepfake films to combat terrorist groups, while also advising governments to exercise extreme caution, use deepfake technology sparingly, and establish a deepfake code of conduct.[2] However, the use of AI in forensic investigations does not come without its challenges such as evidence tampering. From creating hyper-realistic deepfakes i.e. “Deepfake is a form of artificial intelligence (AI) that can be used to create convincing hoax images, sounds, and videos. The term "deepfake" combines the deep learning concept with something fake. Deepfake compiles hoaxed images and sounds and stitches them together using machine learning algorithms. As a result, it creates people and events that do not exist or did not actually happen. It is most notably used for nefarious purposes, such as to mislead the public by spreading false information or propaganda or to mislead the courts on the track which is far from justice. For example, an AI generated video could show a world leader or celebrity saying something seditious, which in reality they have not said, and can be used as an evidence against them in the court to prove a something they have not actually committed. also referred to as “fake news” that shifts public opinion.” [3] to manipulating digital evidence, AI has introduced new dimensions of criminality, testing the resilience of legal frameworks both

[1] Desk TC, “Pune Porsche Crash: Police to Digitally Recreate Accident Scene with AI Tools”, available at <https://timesofindia.indiatimes.com/city/pune/pune-porsche-crash-police-to-digitally-recreate-accident-scene-with-ai-tools/articleshow/110549050.cms> (January 15, 2025).

[2] Northwestern Buffett Institute for Global Affairs, “The Rise of Artificial Intelligence and Deepfakes”, available at <https://buffett.northwestern.edu/documents/buffett-brief_the-rise-of-ai-and-deepfake-technology.pdf> (July 2023).

[3] Fortinet, “What is a Deepfake?”, available at <https://www.fortinet.com/resources/cyberglossary/deepfake> (January 10, 2025).

globally and nationally. This paper evaluates AI crimes such as evidence tampering through AI-generated tools such as machine learning algorithm, facial recognition algorithm, etc. This paper shall also explore the dynamics of the other countries and thus, concluding the paper with critically analyzing the need for advanced forensic tools to detect these algorithms and also recommending to bring some changes into current legislative frameworks like Bharatiya Sakshya Adhiniyam 2023, IT Act, 2000 and punishment of evidence tampering under Bharatiya Nyaya Sanhita, 2024 as it is need of an hour with growing complexities into the criminal justice system. Let's first understand what digital evidences are under various legal framework before delving into our main issue as in how AI tampers these evidences.

EVIDENCE AND DIGITAL EVIDENCES

“"Evidence" means and includes--

(i) All statements, including those supplied electronically, that the Court authorizes or compels witnesses to make before it in respect to questions of fact under investigation are referred to as oral evidence.

(ii) All documents submitted for the Court's scrutiny, including electronic or digital records, are referred to as documentary evidence. [4] *”* under section 2(e) of The Bharatiya Sakshya Adhiniyam (BSA), 2023.Further the act expands the evidentiary value of digital evidence by considering it as primary evidence under section 57 of the act and has provided more importance in legal proceedings. It is stated as following under the act, “ *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, Where an electronic or digital record is produced from proper custody, such electronic and digital record is primary evidence unless it is disputed, 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, 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”* [5]Also under section 79A of IT Act, 2000 defines electronic or digital evidence and states that it may be presented before court or any other authority as proof and also defines what constitutes “electronic form evidence” i.e. Any information of probative value that is

[4] Bharatiya Sakshya Adhiniyam of 2023 section 2(e).

[5] Bharatiya Sakshya Adhiniyam of 2023 section 57.

either kept or communicated in electronic form, including computer evidence, digital audio, digital video, cell phones, and digital fax machines. [6] The most common types of digital evidences can be grouped into five categories i.e. 1. Communications data (text messages, video and audio calls);2. Transactional data (records of online transactions); 3. Cloud storage data (ex. Google drive or One drive); 4. Social media content; 5. Web browser history. Digital evidences are considered to be less tangible and highly volatile and thus, it is generally believed that it is easier to tamper digital evidences than physical evidences as digital evidences are basically derived from physical evidences only.

EVIDENCE TAMPERING AND AI

So what does it exactly mean by evidence tampering?

Tampering with evidence, also known as evidence tampering, involves altering, concealing, falsifying, or destroying evidence to hinder an investigation by law enforcement, government, or regulatory authorities.[7] This is also referred to as tampering of evidence in civil cases. Digital evidence tampering can be difficult to detect, as little modifications can have a significant impact on the verdict. Constantly comparing digital evidence with copies to identify tampering may not be practically possible as this requires a lot of resources such as additional security infrastructure and personnel. Under Section 238 of the Bharatiya Nyaya Sanhita, 2023, it is a criminal offence for any individual who knows or has reason to believe that a crime has been committed to deliberately hide evidence or provide false information to shield the offender. The prescribed penalties are as follows: (a) If the underlying offence is punishable by death, the individual may face imprisonment for up to seven years along with a fine. (b) If the primary offence carries a life sentence or a maximum punishment of ten years, the offender may be imprisoned for up to three years and subjected to a fine. (c) If the offence is punishable by a prison term of less than ten years, the individual may face up to one-fourth of the maximum sentence, a fine, or both. Tampering with digital evidence may involve compromising digital fingerprints or manipulating movies, texts, and audios to make them appear more real and legitimate than they are, employing modern technology such as AI. In the field of criminal law, the use of technology is not a novel concept, over the past few years they share close bond such as Fingerprint analysis changed investigations in the late 19th century.

[6] Ganguli, Prithwish, “Admissibility of Digital Evidence under Bharatiya Sakshya Sanhita: A Comparative Study with the Indian Evidence Act”, available at SSRN: <https://ssrn.com/abstract=4977238> (October 06, 2024).

[7] Chris William Sanchirico, “Evidence Tampering”, Duke Law Journal Vol.53, 1215-1336 (2004).

It gave investigators a reliable way to link suspects to crime scenes, Automated systems like AFIS in the 20th century made the process faster and more efficient. In the 1920s, Calvin Goddard's comparison microscope transformed ballistics by helping investigators match bullets to firearms. Modern tools like IBIS now deliver even quicker and more precise results. Radio communication improved coordination among officers. The American Academy of Forensic Sciences, founded in 1948, brought forensic science to more police departments. Dash and body cameras protect officers and provide critical evidence, improving transparency and accountability. [8]Artificial Intelligence (AI) is a field of study focused on creating computers and machines capable of thinking, learning, and performing tasks that typically require human intelligence or involve processing vast amounts of data beyond human capacity. AI encompasses a range of technologies, including machine learning and deep learning, which are utilized for data analysis, predictive modelling, object recognition, natural language processing, recommendation systems, intelligent information retrieval, and various other functions. AI is revolutionizing criminal justice system which has various setbacks, like evidence tampering being discussed in this paper through its systems and algorithms. So, let's find out how AI systems works in tampering of evidence?

EVIDENCE TAMPERING THROUGH AI TOOLS AND SYSTEMS

The capabilities of AI can effortlessly pull someone into an event in which someone has not even participated, imagine the impact of this on an criminal trial, when such technology is used to tamper with the evidence. [9]Earlier, AI tools like Photoshop, Canva etc were used to tamper with visual evidences which operate on machine learning like generative fill and neutral networks. However, the results produced by such tools are distinguishable and can be detected. In the recent times, with the development in AI technology and advances in machine learning, has resulted in AI giving hyper realistic results which are hardly distinguishable from the reality. These tools in order to give such results uses deep neutral networks (DNNs) which is a type of machine learning model that is designed to impersonate human brain. This, while tampering with the evidence take the form of a face swap, voice alteration or digital signature forgery. [10]A deep neural network (DNN) consists of multiple hidden layers and serves as the

[8] Northern Michigan University, “Technology and Criminal Justice: The Impact on Criminal Investigation” available at <https://online.nmu.edu/technology-and-criminal-justice/> (June 28, 2023).

[9] Shubham Handa and Shailja Thakur, “Role of Artificial Intelligence in Admissibility of Electronic Evidence”, International Journal of Research Publication and Reviews Vol. 5,1323-1328 (November, 2024).

[10] K. Alhosani and SM. Alhashmi, “Opportunities, Challenges, and Benefits of AI Innovation in Government Services: A Review”, available at <https://doi.org/10.1007/s44163-024-00111-w> (04th March 2024).

foundation for various deep learning architectures. These architectures are specifically designed for tasks such as image, video, and speech processing. A significant breakthrough occurred in 2014 with the introduction of generative adversarial networks (GANs) and variational autoencoders (VAEs), which revolutionized the field of deep learning. [11]These tools work by identifying and encoding large amount of data and patterns after which it uses that information to produce new hyper realistic content. This tools can not only edit or alter, but they can also in fact generate a new content with the use of specialized algorithms. There are two types of algorithms first is a generator and other is the discriminator. [12]The generator creates a data base based on the desired output, resulting in phony material, while the discriminator evaluates how realistic the initial content is. This process is repeated, allowing the machine to improve at providing realistic content and its discriminator to become more adept at identifying errors for the generator to fix.[13] When utilized in the context of evidence, such technologies and tools have the capability to generate, modify, and manipulate digital evidence. The application of AI in this manner facilitates the commission of serious criminal offences by making evidence tampering more accessible and sophisticated. This includes fabricating text messages and computer documents, altering CCTV footage, and modifying images, audio recordings, and other digital evidence. While evidences are meant to guide the court towards the justice, the capabilities of such AI tools poses a serious threat to the integrity, accountability and reliability of digital evidence. The ability of AI to modify or fabricate evidence raises serious concerns about the credibility of digital evidence in judicial proceedings. A judicial system relies heavily on the authenticity and reliability of evidence to ensure fair trials. If courts begin to doubt the integrity of digital evidence, it could erode trust in the justice system, making it difficult to deliver justice fairly and effectively. This, in turn, impacts the procedural rights of defendants, as they may face false or manipulated evidence, making it harder to defend themselves. Without a strong mechanism and a legal framework to regulate the use of AI into the legal realm and to differentiate authentic evidence from AI-generated fabrications, wrongful convictions and miscarriages of justice become a looming threat.

[11] Rohit Tahsildar Yadav, "AI-Driven Digital Forensics", International Journal of Scientific Research & Engineering Trends Volume 10,1673-1681 (2024).

[12] Ibid

[13] Ibid

LEGAL FRAMEWORK

With the development of AI technology countries have taken significant steps to formulate framework to regulate the use of AI in order to prevent misuse of such technology.

Global Legal Framework

EU's introduction of first ever specific law for regulating AI called AI act, even though the act won't be enacted till mid 2025 leaving room for further technology advancement, EU has set a benchmark for other countries.[14] The policy of EU through this regulation have taken significant step in regulating deep fakes by firstly mandating chatbots and AI software's that manipulates images and videos to make sure that people know that it is created by AI. Additionally, the EU's policy includes outright on some practices such as such as the indiscriminate scraping of images[15], adoption of risked based approach and imposing of fine on companies that violate safety regulations.

This EU's regulation is being closely observed by the global leaders. Other than EU, other countries like US, China, Australia have also been on the forefront on formulating framework for regulating the use of AI. Government of US has recently instead of a single law, proposed a number of different laws addressing different AI systems in various sectors. [16] Canadian legislation is also considering a specific law on AI, similarly like EU. Australia, last year ran a public consultation of safe and ethical use of AI in Australia, after which a team of experts was formed to formulate to country's AI laws. On the other hand China has adopted aggressive approach for regulating AI's use, the Chinese government has issued a set of targeted and binding laws, marking some of the first significant measures by an AI power to manage one of the most revolutionary technologies of our time. These restrictions specifically target recommendation algorithms, deep synthesis, generative AI, and, most recently, facial

[14] Ibid

[15] Desk TN, "As European Union Passes World's First Law to Curb Artificial Intelligence, India Set on Different Approach",<http://timesofindia.indiatimes.com/articleshow/105859769.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst> (December 9, 2023).

[16] Economic Times, "A World-First Law in Europe Is Targeting AI. Other Countries Can Learn from It", available at https://economictimes.indiatimes.com/tech/artificial-intelligence/a-world-first-law-in-europe-is-targeting-ai-other-countries-can-learn-from-it/articleshow/112546075.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst (August 15, 2024).

recognition.[17] China is presently considering whether to develop a comprehensive national AI law that may be developed and implemented in the coming years.

Indian Legal Framework

As of now, India does not have a specific law or policy regulating AI, however India aims to formulate ‘AI for all’ which aspire to align with global ethical standards to promote the moral and responsible use of AI across different sector. [18]About digital evidence, currently Sec 61[19] of BSA (replacement of Indian Evidence Act) talks about electronic or digital evidence, and the admissibility of such evidence in defined in Sec 63 of BSA. Furthermore, Sec 81,[20] Sec 85,[21] Sec 86, [22] Sec 87, [23] Sec 90,[24] Sec 93[25] describes different types of digital evidence. Additionally, under- IT act 2000, under Sec 4[26] and Sec 5[27] provides legal recognition to digital records These sections ensure that electronic records and signatures receive the same legal recognition as their physical counterparts. According to these provisions, no legal document or information can be denied validity or enforceability solely because it exists in electronic form. Any requirement under the law for information to be in writing, typewritten, or signed is satisfied if such information or signature is available in electronic format, provided it remains accessible for future reference. This means that electronic records are fully admissible in legal proceedings, and electronic signatures can be used to authenticate such records. Moreover, Sec 65 recognizes tampering with digital documents as an offence. India being a developing country. [28] Even though India’s current legal framework including legislation’s Bharatiya Sakshya Adhiniyam and Information Technology Act provides a underlying approach to digital evidence, however it lacks specific AI governance mechanisms. India while framing the AI for all policy should consider best of all other countries just like India did during the framing of Constitution of India. India requires a multi-dimensional strategy to tackle with the problem of

[17] Fiscal Note, “China’s AI Policy and Development”, available at <https://fiscalnote.com/blog/china-ai-policy-development-what-you-need-to-know> (August 2024).

[18] PIB, “UNESCO and the Ministry of Electronics and Information Technology, Host Multi-Stakeholder Consultation on Safety and Ethics in Artificial Intelligence (AI)”, available <https://pib.gov.in/PressReleasePage.aspx?PRID=2073920> (2024).

[19] Bharatiya Sakshya Adhiniyam of 2023 section 61.

[20] Bharatiya Sakshya Adhiniyam of 2023 section 81.

[21] Bharatiya Sakshya Adhiniyam of 2023 section 85.

[22] Bharatiya Sakshya Adhiniyam of 2023 section 86.

[23] Bharatiya Sakshya Adhiniyam of 2023 section 87.

[24] Bharatiya Sakshya Adhiniyam of 2023 section 90.

[25] Bharatiya Sakshya Adhiniyam of 2023 section 93.

[26] Information Technology Act 2000, section 4.

AI and evidence tampering. Firstly, while establishing a national AI policy dealing with challenges by AI while addressing evidence tampering risks. The policy must mandate compulsory verification of digital evidence by advanced technologies like block-chain verification, quantum computing and devices which can detect AI algorithms. The purposed policy should also mandate development of forensic device developed on AI system trained on extensive data base comprising of authentic & tampered media. This will expose it numerous algorithms allowing it learn and identify the difference between real and manipulated content, enabling a sophisticated forensic analysis. This way explores AI’s potential for self-regulations by creating AI detection mechanism that can differentiate between original evidence and artificially generated evidence. The proposed policy should be formulated in a way that it addresses the current issues as well as it is flexible to adopt with the future technological innovations.

POSSIBLE SOLUTIONS

In the light of above stated issue regarding evidence tampering, India has ever since been paranoid about the technological advancements and find it difficult to accept new technological advancements, which has always given an undue advantage to the wrongdoers. Indian policy makers must prioritize developing a extensive AI regulatory framework just like EU’s Artificial Intelligence Act and China’s Generative AI Regulation which aims to address technological risks and governs the use of AI within its territory. India’s current legal framework including legislation’s Bharatiya Sakshya Adhiniyam, Bharatiya Nyaya Sanhita and Information Technology Act provides a underlying approach to digital evidence, however it lacks specific AI governance mechanisms. Also, India is taking steps when it comes to collaborative efforts with other global technological leaders towards AI development for example US India Artificial Intelligence (USIAI) Initiative, Indo-German Science and Technology Centre, also India has become member of Global Partnership on AI, and as we acknowledge the significance of active participation of India with other global countries to develop better AI technology, India in collaboration with other countries should also take steps in regulating such technologies, because when left unregulated such technology can contribute to criminal activities such as evidence tampering, cyber fraud, etc. By actively addressing AI's potential for evidence manipulation, India can transform a potential technological challenge into a sophisticated system of digital authentication and forensic reliability.

CONCLUSION

In conclusion, the rapid advancement of Artificial Intelligence (AI) has revolutionized forensic investigations and legal proceedings, offering tools for digital reconstruction, predictive analytics, and enhanced evidence processing. However, its potential for evidence tampering, particularly through deepfakes, digital alterations, and fabricated records, poses a serious threat to judicial integrity. Without proper safeguards, AI-driven manipulation of evidence could lead to wrongful convictions and miscarriages of justice, eroding trust in digital evidence and compromising defendants' procedural rights. Recognizing these risks, several global legal frameworks, including the EU’s AI Act, the US’s sectoral AI regulations, and China’s stringent AI governance, have taken proactive steps to address AI misuse. However, India lacks a dedicated AI-specific regulatory framework. Existing laws, such as the Bharatiya Sakshya Adhiniyam, the IT Act, and the Bharatiya Nyaya Sanhita, provide foundational support but do not comprehensively address AI-driven evidence manipulation. To counter these threats, India must urgently adopt a multi-dimensional approach, including legislative reforms, forensic AI detection mechanisms, judicial training, and international collaboration. By integrating advanced AI verification tools and global regulatory cooperation, India can harness AI’s potential while safeguarding its justice system from technological exploitation, ensuring fairness and accountability in the digital era.

BIBLIOGRAPHY

- https://3384_08.%20Seng%20&%20Mason%20%20Artificial%20Intelligence%20and%20Evidence.pdfethics7.pdf
- https://blog.ipleaders.in/all-aboutdigitalevidence/#Information_Technology_Act_2000
- https://doi.org/10.1016/j.fsidi.2020.300924
- https://economictimes.indiatimes.com/tech/artificial-intelligence/a-world-first-law-in-europe-is-targeting-ai-other-countries-can-learn-from-it/articleshow/112546075.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst
- https://jatheon.com/blog/digital-evidence-examples/
- https://link.springer.com/article/10.1007/s44230-024-00074-2
- https://pib.gov.in/PressReleasePage.aspx?PRID=2073920
- https://www.researchgate.net/profile/Greg-Marston/publication/241578701_Tampering_With_the_Evidence_A_Critical_Appraisal_of_Evidence-Based_PolicyMaking/links/02e7e53a28317f2a45000000/Tampering-With-the-Evidence-A-Critical-Appraisal-of-Evidence-Based-PolicyMaking.pdf
- https://www.unodc.org/e4j/zh/cybercrime/module-6/key-issues/handling-of-digital-evidence.html
- https://www.verylaw.com/blog/is-tampering-with-evidence-a-serious-crime/
- International Journal of Research Publication and Reviews, Vol (5), Issue (11), November (2024), Page – 1323-1328
- Paul W. Grimm, Maura R. Grossman, and Gordon V. Cormack, Artificial Intelligence as Evidence, 19 NW. J. TECH. & INTELL. PROP. 9 (2021).
- Sabine Gless, Frederic Lederer, & Thomas Weigend, AI-Based Evidence in Criminal Trials?, 59 Tul