



**East African Journal of Law and Ethics**

[eajle.eanso.org](http://eajle.eanso.org)

**Volume 7, Issue 1, 2024**

**Print ISSN: 2707-532X | Online ISSN: 2707-5338**

Title DOI: <https://doi.org/10.37284/2707-5338>



EAST AFRICAN  
NATURE &  
SCIENCE  
ORGANIZATION

*Original Article*

## **Legal and Practical Challenges for the Admissibility of Artificial Intelligence (AI) Evidence in Criminal Proceedings in Mainland Tanzania**

*Verus Cronery Rwetembula*<sup>1\*</sup>

<sup>1</sup> Court of Appeal of Tanzania, P. O. Box 9004, Dar Es Salaam, Tanzania.

\* Author's Email: [verus.rwetembula@judiciary.go.tz](mailto:verus.rwetembula@judiciary.go.tz)

**Article DOI: <https://doi.org/10.37284/eajle.7.1.2431>**

### **Date Published: ABSTRACT**

21 November 2024

#### **Keywords:**

*Admissibility,  
Artificial Intelligence,  
Criminal Justice,  
Evidence,  
Technological  
Advancement.*

This article investigates the admissibility of artificial intelligence (AI) evidence in criminal proceedings within Mainland Tanzania. As AI technologies increasingly generate data that could be used in legal contexts, questions arise regarding the reliability, transparency, and potential biases inherent in AI-based evidence. The Tanzanian legal framework, including the Evidence Act and the Electronic Transactions Act, lacks explicit provisions for AI-generated evidence, which creates challenges for its integration into criminal cases. This paper explores current admissibility standards in Tanzania, analyzing how AI evidence could be evaluated for relevance and probative value under existing laws. By examining principles such as legal positivism and reliability theory, and drawing on international insights, the article proposes interpretative approaches to assess AI evidence's validity and reliability in Tanzanian courts. Ultimately, this study seeks to provide insights and recommendations for Tanzanian legal professionals and policymakers, aiming to support the development of clear guidelines for the use of AI in the criminal justice system and ensure that technological advancements uphold procedural fairness and justice.

#### **APA CITATION**

Rwetembula, V. C. (2024). Legal and Practical Challenges for the Admissibility of Artificial Intelligence (AI) Evidence in Criminal Proceedings in Mainland Tanzania. *East African Journal of Law and Ethics*, 7(1), 136-148. <https://doi.org/10.37284/eajle.7.1.2431>

#### **CHICAGO CITATION**

Rwetembula, Verus Cronery. 2024. "Legal and Practical Challenges for the Admissibility of Artificial Intelligence (AI) Evidence in Criminal Proceedings in Mainland Tanzania." *East African Journal of Law and Ethics* 7 (1), 136-148. <https://doi.org/10.37284/eajle.7.1.2431>.

#### **HARVARD CITATION**

Rwetembula, V. C. (2024) "Legal and Practical Challenges for the Admissibility of Artificial Intelligence (AI) Evidence in Criminal Proceedings in Mainland Tanzania.", *East African Journal of Law and Ethics*, 7(1), pp. 136-148. doi: 10.37284/eajle.7.1.2431.

#### **IEEE CITATION**

V. C., Rwetembula. "Legal and Practical Challenges for the Admissibility of Artificial Intelligence (AI) Evidence in Criminal Proceedings in Mainland Tanzania.", *EAJLE*, vol. 7, no. 1, pp. 136-148, Nov. 2024.

## MLA CITATION

Rwetembula, Verus Cronery. "Legal and Practical Challenges for the Admissibility of Artificial Intelligence (AI) Evidence in Criminal Proceedings in Mainland Tanzania." *East African Journal of Law and Ethics*, Vol. 7, no. 1, Nov. 2024, pp. 136-148, doi:10.37284/eajle.7.1.2431.

## INTRODUCTION

The growing integration of artificial intelligence (AI) into various sectors has brought about significant changes, particularly in how information is generated, processed, and used as evidence in criminal proceedings.<sup>1</sup> AI has the potential to analyze vast amounts of data, assist in crime prediction, and even contribute to the identification of suspects through facial recognition and other forms of digital analysis. However, its use as evidence in court presents a unique set of challenges, especially in the context of Mainland Tanzania, where legal frameworks have yet to fully address AI's impact on evidentiary standards.<sup>2</sup>

Globally, concerns have been raised about the reliability and fairness of AI-generated evidence, particularly given the potential biases embedded in algorithms used to process data. Scholars like Cathy O'Neil argue that many algorithms are inherently biased, potentially leading to wrongful convictions if unchecked.<sup>3</sup> Furthermore, AI evidence often lacks transparency, as it is typically processed by proprietary systems, meaning that even experts may not fully understand how certain conclusions are reached. These factors call into question the reliability and probative value of AI evidence, which are key components of admissibility in many legal systems.<sup>4</sup>

Legal positivism, as espoused by H.L.A. Hart, suggests that the legitimacy of laws, and by extension the rules of evidence, derives from social facts and accepted practices rather than moral content. Hart's theory implies that if AI

evidence is to be used in court, it must be governed by established legal standards and recognized as a valid source of information within the legal system.<sup>5</sup> Thus, for Tanzanian courts to admit AI evidence in criminal cases, it is crucial to have a clear legal framework that acknowledges both the capabilities and limitations of AI technologies. This paper examines the admissibility of AI-generated evidence in criminal proceedings in Mainland Tanzania, focusing on the potential gaps and implications within existing Tanzanian law.

## Guiding questions

As AI-generated evidence becomes more prevalent, courts face pressing questions such as: How should they evaluate the reliability and authenticity of evidence produced by AI? Can traditional evidentiary criteria sufficiently address the unique attributes of AI, such as algorithmic opacity, potential biases, and "black box" processes?<sup>6</sup> These challenges underscore the need for legal reform and judicial insight into the specific nature of AI evidence to ensure its fair and effective use within Tanzanian criminal law. As the literature doubts, the researcher also have similar questions and worries on the integration of AI evidence in the legal system as to;

What are the current legal standards for admissibility of evidence in criminal proceedings in Mainland Tanzania, and how do they apply to AI-generated evidence?

How does AI evidence meet (or fail to meet) traditional criteria of relevance, probative value, and reliability under Tanzanian law?

<sup>1</sup> Grimm, P. W., et al, "Artificial Intelligence as Evidence" 19, *Northwestern Journal of Technology and Intellectual Property*, 2021, pp. 9-106.

<sup>2</sup> Lee, R., "The Inaccuracies of AI in Facial Recognition: Implications for Criminal Trials", 11, *Journal of Technology & Sociology*, 2020, pp. 23- 36, p.26.

<sup>3</sup> O'Neil, C., *"Weapons of Math Destruction"*, Crown, 2016.

<sup>4</sup> Hart, H., *"The Concept of Law"*, (3rd edn), OUP, 2012.

<sup>5</sup> *ibid*

<sup>6</sup> Ngowi, T., "Data Input and the Reliability of AI Systems in Criminal Forensics", 7, *African Digital Law Journal*, 2022, pp. 44-56, p. 49.

What are the primary challenges of integrating AI-generated evidence in Tanzanian criminal courts, particularly concerning issues of transparency, bias, and algorithmic reliability?

### **The concepts of admissibility, AI and AI-generated evidence, and criminal proceedings**

#### **Artificial intelligence**

Eftychia argues that Artificial intelligence (AI) systems are software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behavior by analyzing how the environment is affected by their previous actions. As a scientific discipline, AI includes several approaches and techniques, such as machine learning (of which deep learning and reinforcement learning are specific examples), machine reasoning (which includes planning, scheduling, knowledge representation and reasoning, search, and optimization), and robotics (which includes control, perception, sensors and actuators, as well as the integration of all other techniques into cyber-physical systems).<sup>7</sup>

#### **Artificial intelligence evidence**

Artificial Intelligence evidence refers to information or data generated, processed, or analyzed by artificial intelligence systems that can be used to support claims, conclusions, or decisions in various contexts.<sup>8</sup> This type of

evidence can arise from AI's capabilities in areas such as data analysis, pattern recognition, and decision-making. In so far as AI evidence is concerned, it is typically based on large datasets that AI systems analyze to identify trends, patterns, or insights. AI is capable of analyzing vast amounts of data quickly, making it possible to gather evidence from diverse and extensive sources. Ordinarily the processes and algorithms used to generate AI evidence should be understandable and explainable to ensure reliability and its usefulness depends on its relevance to the specific problem or question at hand. Apart from the fact that AI can analyze documents or predict outcomes, providing evidence for legal arguments, AI evidence leverages the capabilities of artificial intelligence to provide data-backed insights that can aid in decision-making across various fields. Techniques from artificial intelligence (AI) can be used in forensic evidence evaluation and are currently applied in biometric fields. However, it is generally not possible to fully understand how and why these algorithms reach their conclusions<sup>9</sup>.

#### **Admissibility**

On the other hand, admissibility pertains to whether evidence can be considered by a court or other decision-making body. For evidence to be admissible, it must meet certain criteria established by legal rules or standards. Evidence may be deemed admissible based on factors such as relevance, reliability, authenticity, and compliance with procedural rules. In so far as our laws and legal system is concerned, admissibility of evidence purely depends on the determination of the trial judge or magistrates.<sup>10</sup> In other words, it is upon the court to assess whether at a given circumstance, based on the material facts and

<sup>7</sup> Bampasika, E., "Artificial Intelligence as Evidence in Criminal Trial", Doctoral Researcher, Member of the Otto Hahn Research Group on Alternative Criminal Justice Max Planck Institute for the Study of Crime, Security and Law Günterstalstraße 73, 79100, available at <[e.bampasika@csl.mpg.de](mailto:e.bampasika@csl.mpg.de)>, (accessed 4<sup>th</sup> October, 2024).

<sup>8</sup> Gless, S., Lederer, I.F., and Weigend, T. "AI-Based Evidence in Criminal Trials?", 59, *Tulsa Law Review*, 2024, pp. 1-37.

<sup>9</sup> Durán, J.M., *et al.*, "From understanding to justifying: computational reliabilism for AI-based forensic evidence evaluation", *Forensic Science International: Synergy*, 9, 2024, p.100554.

<sup>10</sup> Genty, E., "The Challenges of integrating AI-generated Evidence into the Legal system", 2024, available at <<https://www.akerman.com>> (accessed 17th August 2024).

prevailing situations of a case, determine whether a relevant evidence may be admissible or not.

The law however provides for circumstances where the facts are considered admissible or said to be proved. It inter alia provides as follows; ‘A fact is said to be proved when- (a) in criminal matters, except where any statute or other law provides otherwise, the court is satisfied by the prosecution beyond reasonable doubt that the fact exists; (b) in civil matters, including matrimonial causes and matters, its existence is established by a preponderance of probability.

### **Criminal proceedings**

Criminal proceedings refer to the legal process through which individuals accused of committing a crime are prosecuted and adjudicated in a court of law. Generally criminal proceedings is a process which involves criminal investigation, arrest of criminal suspects and accused persons, preparation of charge, Initial appearance, preliminary hearing or arraignment, pre-trial motions, trial, verdict, sentencing and appeals in criminal cases. Each stage has specific procedures and rights to ensure a fair trial, influenced by legal standards and constitutional protections. Some authors argue that it is conceivable that criminal proceedings cause psychological harm to the crime victims involved, that is, cause secondary victimization.<sup>11</sup>

### **Legal framework governing admissibility of evidence in mainland Tanzania**

The integration of AI evidence in Tanzanian criminal proceedings is guided by existing laws focused on evidence, electronic transactions, cybersecurity, and data protection. In Tanzania, the application of AI evidence in judicial proceedings is influenced by various laws and regulations as follows;

### **The Evidence Act, Cap 6 R.E 2022**

The Act establishes foundational principles that govern the admissibility and relevance of evidence in judicial proceedings to include artificial intelligence (AI) evidence. The Act provides a framework for determining the relevance of AI evidence in judicial proceedings by emphasizing the importance of connection to the facts, reliability, and admissibility standards.<sup>12</sup>

Under Section 7 the Act states that evidence is relevant if it makes a fact in issue more or less probable. AI evidence must therefore be shown to directly relate to the facts of the case. For example, if AI analyzes data to identify patterns relevant to a fraud case, it can be considered relevant. Under the admissibility criteria for AI evidence, Section 8 of the Act stipulates that for evidence to be admissible, it must be relevant. Therefore, any AI evidence presented in court must demonstrate its direct connection to the legal issues at stake. This relevance criterion ensures that AI evidence contributes meaningfully to the case.<sup>13</sup> Regarding the weight of evidence, the Act allows the court to consider the weight of evidence. Even if AI evidence is deemed relevant, its probative value may be assessed based on how accurately it reflects the facts of the case. Courts may require expert testimony to establish the reliability of the AI processes used.<sup>14</sup>

Similarly AI-generated reports or data can be classified as documentary evidence defined under Section 3 read together with Section 67 of the Act. The Act outlines how such documents must be authentic and reliable to be admissible, impacting their relevance. The Act grants judge’s discretion to determine what evidence is relevant and admissible.<sup>15</sup> This means that judges can evaluate AI evidence based on its context and the quality of the data or algorithms involved. AI evidence must be accompanied by assurances of its

<sup>11</sup> Orth, U., “Secondary victimization of crime victims by criminal proceedings”, *Social justice research*, 15, 2002, pp. 313-25.

<sup>12</sup> Archak, D., “AI in Legal Evidence Analysis: Ethical and Legal Implications”, 2(7), *International Journal for Legal Research and Analysis*, 2024.

<sup>13</sup> Archak, D., (n. 12)

<sup>14</sup> Genty, E., (n.10).

<sup>15</sup> Zafar, A., “Balancing the Scale: navigating ethical and practical challenges of AI integration in legal practice” 2024, available at <<https://link.springer.com>> (accessed 28th October 2024).



reliability and authenticity, especially if it involves complex algorithms.<sup>16</sup> The court will assess whether the AI methods used are widely accepted in the relevant field and whether they meet standards of scientific validity. As AI technologies continue to develop, the application of these principles will be critical in ensuring that AI evidence is effectively integrated into the Tanzanian legal system.<sup>17</sup>

### **The Electronic Transactions Act, Cap 442 R.E 2022**

The Act provides a legal framework for the use of electronic records and communications, which is particularly relevant when considering artificial intelligence (AI) evidence in criminal proceedings.<sup>18</sup>

Under Section 3 the Act recognizes electronic records as having legal validity. This is crucial for AI-generated evidence, which often exists in digital form. If AI outputs are presented in court, they can be recognized as valid evidence, provided they meet the necessary legal criteria. Similarly, regarding the admissibility of electronic evidence, the stipulations of Section 10 clearly outline the conditions under which electronic records can be admissible in court.<sup>19</sup> It states that such records are admissible as evidence if they are relevant and have not been tampered with. Artificial Intelligence evidence, when presented as electronic records, must demonstrate its relevance to the case at hand.<sup>20</sup>

Under the stipulations of Section 11, the Act also sets emphasis on the issues of integrity and authenticity as it provides for the importance of maintaining the integrity of electronic records. Artificial Intelligence evidence must be shown to be authentic and reliable, meaning the processes and algorithms used to generate this evidence should be transparent and trustworthy. This directly impacts its relevance, as evidence that lacks authenticity may be deemed irrelevant.

Under Section 12, however, the Act creates a presumption that electronic records are accurate unless proven otherwise. This presumption can support the relevance of AI evidence, as it implies a level of trust in the data and outputs generated by AI systems, provided they adhere to the legal standards established.

Under Section 5, the Act recognizes electronic signatures, which may be relevant when AI systems generate documents or reports that require authentication. The ability to authenticate AI-generated evidence through electronic signatures adds to its relevance in legal contexts. On top of that it also complements data protection laws, ensuring that AI systems handling personal data comply with legal standards. If AI evidence involves personal or sensitive data, its relevance must be assessed in light of compliance with privacy regulations, thus influencing how it is treated in court.<sup>21</sup>

The Act provides a crucial legal foundation for the admissibility and relevance of AI evidence in Tanzanian criminal proceedings. By recognizing electronic records, ensuring integrity, and setting standards for electronic evidence, the Act supports the effective integration of AI technologies into the legal framework, enhancing the ability to utilize AI-generated data in a meaningful way in court.

### **The Cybercrimes Act, No 14 of 2015**

The Act establishes a legal framework for addressing issues related to cybercrime and electronic evidence. Its provisions are particularly relevant when considering the relevance of AI evidence in judicial proceedings.

The Act recognizes the legitimacy of electronic evidence, including data generated or processed by AI systems. This legal recognition is essential for AI evidence to be considered relevant in court. The Act also addresses concerns about the

<sup>16</sup> *Ibid.*

<sup>17</sup> Allen, *et al*, Reforming the law of evidence of Tanzania (part two): conceptual overview and practical steps, 32(1), *Boston University International Law Journal*, 2013 pp. 1-53

<sup>18</sup> *Ibid* at p. 15.

<sup>19</sup> Zafar, A. (n. 15).

<sup>20</sup> Handa, S and Thakur, S., "Role of AI in Admissibility of Electronic Evidence", 5(11), *International Journal of Research Publication and Reviews*, 2024, pp. 1323-8.

<sup>21</sup> Allen, *et al.*, (n.12).

integrity of digital evidence and sets standards for proving the authenticity of electronic evidence. AI-generated evidence must be protected against unauthorized access or alterations.<sup>22</sup> If the evidence is shown to be tampered with, it may lose its relevance in court. AI outputs must be accompanied by assurances regarding their origin and the methods used to produce them, enhancing their relevance to the case.

In so far as cybersecurity measures are concerned, the Act emphasizes the need for cybersecurity measures to protect data. If AI evidence is collected from secure systems, its relevance is reinforced, as it indicates a lower likelihood of tampering or error. The Cybercrimes Act intersects with data protection principles. AI evidence that involves personal data must comply with relevant laws, such as the Personal Data Protection Act.<sup>23</sup> This compliance affects its relevance, as courts may evaluate whether the evidence was obtained lawfully and ethically.

With regards to the prevention of Cybercrimes, the Act defines various cybercrimes, and we understand that AI evidence may play a crucial role in investigations and prosecutions. For example, AI tools used to analyze data breaches or fraud cases can provide relevant evidence that supports legal arguments.<sup>24</sup>

It is very clear that the *Cybercrimes Act* provides a framework that underpins the relevance of AI evidence in criminal proceedings in Tanzania. By recognizing electronic evidence, establishing standards for integrity and authenticity, and emphasizing compliance with data protection laws, the Act supports the effective use of AI-generated data in legal contexts, enhancing its relevance and reliability in court.<sup>25</sup>

## **The Personal Data Protection Act, Cap 44 of 2022**

The Act establishes a framework that significantly impacts the relevance of AI evidence in criminal proceedings in Tanzania. By ensuring that personal data is handled lawfully, transparently, and securely, the Act reinforces the integrity and relevance of AI-generated evidence, thereby supporting its appropriate use in the legal system. It plays a critical role in regulating how personal data is handled, which is especially relevant when considering the use of AI evidence in criminal proceedings.<sup>26</sup>

The Act emphasizes on consent and lawful processing and it mandates that personal data must be collected and processed lawfully, typically requiring consent from the data subject. For AI evidence to be relevant in court, it must be demonstrated that the data used was obtained in compliance with these legal requirements. Similarly, under the data minimization principle, the Act emphasizes that only the necessary data for a specific purpose should be collected. AI evidence must therefore be directly relevant to the legal matter at hand and should not include extraneous or irrelevant data.<sup>27</sup>

For purposes of transparency and accountability, the Act requires data controllers to be transparent about how data is collected and used. In the context of AI evidence, this means that the origins and processing methods of the data must be clearly documented, enhancing the relevance of the AI evidence by ensuring its traceability. With regards to the protection of personal data, should it happen that the AI evidence involves personal data; the Act's provisions on protecting individuals' rights must be followed or adhered to. This includes ensuring that the use of such evidence does not violate privacy rights, which

<sup>22</sup> Unesco, How to determine the admissibility of AI generated evidence in Courts , 2023, available at <<https://www.unesco.org>> (accessed 7th October 2024).

<sup>23</sup> Allen, *et al.*, (n. 12).

<sup>24</sup> The National Prosecutions Service, "Criminal Prosecution Case Manual" 2023, available at <<https://tanzlii.org>>. (accessed 17th October 2024).

<sup>25</sup> *Ibid.*

<sup>26</sup> Art. 5(1) (a) the Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence, available at <<https://www.europarl.europa.eu>> (accessed 28th October 2024)

<sup>27</sup> Das, A., "Artificial Intelligence in Legal Evidence Analysis: Ethical and Legal Implications", 2(7), *International Journal for Legal research and Analysis*, 2024 pp. 1-13

can affect its admissibility and relevance in court. Additionally, the Act grants individuals rights concerning their personal data, such as the right to access, rectify, or delete their data. If AI evidence is based on data that infringes these rights, its relevance and acceptability in judicial proceedings may be questioned.<sup>28</sup>

There are also data security measures integrity and reliability, under which the Act mandates that data controllers implement adequate security measures to protect personal data. AI evidence derived from secure and well-protected data sources is likely to be considered more relevant, as it is less susceptible to tampering or loss.<sup>29</sup>

### **The Penal Code, Cap 16 R.E. 2022**

The Act is a crucial legal instrument that defines criminal offenses and the corresponding penalties. It relates to the relevance of AI evidence in criminal proceedings by framing the context within which crimes are defined and prosecuted. AI evidence can play a significant role in clarifying offenses, supporting investigations, and establishing intent, all of which are essential for fair judicial outcomes.<sup>30</sup> The code outlines specific offenses that AI evidence may help to clarify or prove, such as fraud, cybercrime, or other related offenses. AI-generated evidence, like data analysis or predictive algorithms, can be directly relevant in establishing elements of these crimes.<sup>31</sup>

AI may well be used as digital evidence for proving offenses committed under the Penal Code. Given that the Penal Code addresses various crimes that may involve technology (e.g.,

theft, fraud), AI evidence can be crucial in investigations. For instance, AI tools used for digital forensics may analyze electronic communications or financial transactions to uncover criminal activity.<sup>32</sup>

In so far as the question of intent and mental state enshrined under Section 10 of the code is concerned, AI evidence plays a critical role clarifying offenses, supporting investigations, and establishing intent, all of which are essential for establishing the guilt or innocence of the accused. In many offenses, establishing the intent of the accused is crucial. AI systems can analyze behavior patterns or historical data, providing insights into the accused's actions and intentions, thus making AI evidence relevant to determining guilt.<sup>33</sup>

AI technologies can assist law enforcement agencies in collecting and processing evidence related to crimes defined in the code. This includes identifying suspects through data analysis, which can help ensure that relevant evidence is presented in court. The code emphasizes the rights of individuals accused of crimes. AI evidence must be presented in a way that ensures fairness and does not infringe on these rights, thereby affecting its relevance in judicial proceedings.<sup>34</sup>

### **Challenges for the admissibility of AI evidence in criminal proceedings in mainland Tanzania**

The admissibility of Artificial Intelligence (AI) evidence in criminal proceedings in Tanzania is a complex and evolving issue that intersects with legal standards, technological advancements, and

<sup>28</sup> Handa, S and Thakur, S., "Role of AI in Admissibility of Electronic Evidence", 5(11), *International Journal of Research Publication and Reviews*, 2024, pp. 1323-8.

<sup>29</sup> Jada, I., Mayayise, T.O., "The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review" *Data and Information Management*, 2024 available at <[www.journals.elsevier.com/data-and-information-management](http://www.journals.elsevier.com/data-and-information-management)> (accessed 27th October 2024).

<sup>30</sup> Haider, R., Pearl, J., "AI-Driven Cyber Forensics: Investigating Cybercrimes and Strengthening Multi-Factor Authentication in E-Commerce" available at <<https://www.researchgate.net/publication>> (accessed 28th October, 2024).

<sup>31</sup> Dunsin, D., *et al*, "A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response", 2024. available at <<https://www.sciencedirect.com>>, (accessed 28<sup>th</sup> October 2024).

<sup>32</sup> Quezada, K., Vogiatzoglou, P. and Royer, S., "Legal Challenges in Bringing AI Evidence to the Criminal Courtroom", 2021, pp. 1-20.

<sup>33</sup> Dory A.D., Reiling., "Courts and Artificial Intelligence", 11(2), *International Journal for Court Administration*, 2020, pp. 1-10.

<sup>34</sup> *Ibid*.

ethical considerations. In so far as the admissibility of AI evidence in criminal proceedings in Tanzania is concerned, it is a critical area that requires careful consideration and proactive legal reform.<sup>35</sup> As AI technologies become more integrated into the justice system, establishing clear standards for admissibility, reliability, and ethical use is essential. By addressing these challenges, Tanzania can harness the potential of AI while safeguarding the principles of justice and fairness in criminal proceedings.<sup>36</sup>

The traditional principles of admissibility, relevance, and probative value remain foundational in determining what constitutes acceptable evidence in Tanzanian courts. The *Evidence Act*<sup>37</sup> defines admissible evidence and provides guidelines on relevance, but does not explicitly address AI or digital evidence, given its enactment before the widespread adoption of such technologies in the justice sector. Similarly, the *Electronic Transactions Act*<sup>38</sup> which governs electronic data and records, includes provisions on digital evidence but is silent on the specific complexities of AI-generated data, such as algorithmic transparency and potential biases.

### Legal framework

Tanzania's legal framework primarily relies on the *Evidence Act*<sup>39</sup>, which outlines the general principles governing the admissibility of evidence. However, it does not explicitly address AI-generated evidence, something which may create uncertainty about its acceptance in court.<sup>40</sup> As AI technology evolves, there may be a need to amend existing laws or introduce new legislation that specifically addresses the criteria for the

admissibility of AI evidence, ensuring it aligns with international best practices. However, the *Electronic Transaction Act*<sup>41</sup> complement the admissibility of some of electronic evidence, but the same is not sufficiently addresses on the AI regime.

### Criteria for admissibility

Like all evidence, AI-generated evidence must be relevant to the case at hand. It should directly support or contradict claims made by the parties involved.<sup>42</sup> After passing the test or requirement of relevance it must prove reliable before being applied. Courts typically require evidence to be reliable and based on sound principles. The methodologies behind AI algorithms must be transparent and scientifically validated to establish reliability.<sup>43</sup>

Given the technical nature of AI, courts may require expert testimony to explain how the AI operates, its limitations, and the context in which it was used. This can help establish the evidence's credibility.<sup>44</sup> Many jurisdictions including the United Republic of Tanzania lack specific laws and regulations that define the criteria for the admissibility of AI evidence.<sup>45</sup> This ambiguity can lead to inconsistencies in how courts evaluate such evidence. Even the relevant existing laws are sometimes quite outdated. Most countries are suffering the challenge of having outdated legislation that are incapable to cater for the needs and requirements or otherwise demands of the current growing pace of technology. Existing laws may not adequately address the unique characteristics of AI-generated evidence, leading

<sup>35</sup> Grimm, P. W., *et al.*, (n. 1), p. 79.

<sup>36</sup> Kapinga, A., "The Digital Transformation of Tanzania's Criminal Justice System: Opportunities and Challenges", 2024, available at < <https://papers.ssrn.com>.> (accessed 12th July 2024).

<sup>37</sup> Cap 6 R.E. 2022.

<sup>38</sup> No 14 of 2015.

<sup>39</sup> Cap 6 R.E. 2022.

<sup>40</sup> Gless, S., Lederer, I.F., and Weigend, T., "AI-Based Evidence in Criminal Trials", 59, *Tulsa Law Review*, 2024, pp. 1-37.

<sup>41</sup> Cap 442 R.E 2022

<sup>42</sup> Schindler, E., "Judicial system are turning to AI to help manage vast quantities of data and expedite case resolution", published on January, 8, 2024, (accessed on 08, October 2024).

<sup>43</sup> *Ibid*

<sup>44</sup> Sushina, T., "Artificial Intelligent in criminal justice system; leading trends and possibilities, department of criminal procedure", Kutafin Moscow State Law University (MSAL) Vol 4.

<sup>45</sup> Section 64A of the Evidence Act of 2015, for the admissibility of electronic evidence in Tanzania, also Section 18 the Electronic Transaction Act, Cap 442 R.E 2022



to difficulties in its integration into traditional legal standards.<sup>46</sup>

In Tanzania so far there is the absence of AI-specific laws. We are still struggling in as far as having comprehensive IT legal systems and laws are concerned.<sup>47</sup> Tanzania currently lacks comprehensive legislation specifically addressing the use of AI evidence in criminal proceedings. Existing laws may not adequately account for the unique characteristics and challenges associated with AI technologies. The prevalent existing legal framework primarily focuses on traditional forms of evidence and may not fully address the nuances of AI-generated evidence, leading to uncertainty in its admissibility and use in court.<sup>48</sup>

### Admissibility standards

Hitherto there are unclear admissibility criteria. The criteria for the admissibility of AI evidence, including standards for relevance, reliability, and authenticity, are not clearly defined under our laws and procedure. This lack of clarity can lead to inconsistencies in how courts handle AI evidence. Judges may face challenges in assessing the probative value of AI evidence without established guidelines, potentially leading to arbitrary decisions regarding its admissibility.<sup>49</sup>

### Procedural challenges

Integrating AI evidence into existing legal procedures can be complex. Courts may struggle to adapt traditional evidentiary rules to accommodate AI. So far we are not capable of talking of procedural rules that effectively cater for all areas that are technologically related.<sup>50</sup> The *Criminal Procedure Act*<sup>51</sup> for example does not have provisions that are sure of matching the current sweeping change of technology and online

platform issues. In addition to that the admissibility of AI evidence can lead to lengthy appeals and challenges, as parties contest its reliability and relevance, potentially delaying justice.

### Complexity and understanding

The sophisticated nature of AI technologies can create barriers to understanding for judges, lawyers, and juries. This complexity may hinder effective evaluation and interpretation of AI evidence in court. As said earlier, courts may require expert witnesses to explain the workings and implications of AI evidence, which can complicate proceedings and introduce additional variables.<sup>52</sup>

### Data privacy and ethical considerations

The use of AI in gathering evidence, such as surveillance or data mining, raises significant privacy issues. The legal framework must balance the need for effective law enforcement with the protection of individual rights. The administration of AI evidence must also consider ethical implications, including the transparency of AI processes and the accountability of those who utilize these technologies. Courts must navigate these concerns while considering the admissibility of such evidence. The ethical use of AI in legal contexts necessitates careful consideration, including the transparency of AI processes and accountability for outcomes.<sup>53</sup>

### Bias and fairness concerns

The use or application of AI raises a huge possibility or potential for discrimination due to the fact that the AI algorithms can reflect biases present in their training data, raising concerns

<sup>46</sup> Archak, D., "AI in Legal Evidence Analysis: Ethical and Legal Implications", 2(7), *International Journal for Legal Research and Analysis*, 2024.

<sup>47</sup> Adejo, A. A., & Misau, A.Y., "Application of Artificial Intelligence in Academic", 2021.

<sup>48</sup> Zafar, A., "Balancing the Scale: navigating ethical and practical challenges of AI integration in legal practice" 2024, available at <<https://link.springer.com>> (accessed 28th October 2024).

<sup>49</sup> Section 64A of the Evidence Act of 2015, for the admissibility of electronic evidence in Tanzania, also Section 18 the Electronic Transaction Act, Cap 442 R.E 2022

<sup>50</sup> *Ibid*

<sup>51</sup> Cap 20 R.E 2022.

<sup>52</sup> Rizwan, H., & Judea, P., "AI-Driven Cyber Forensics: Investigating Cybercrimes and Strengthening Multi-Factor Authentication in E-Commerce", available at <<https://www.researchgate.net/publication>> (accessed 28th October, 2024).

<sup>53</sup> Schindler, E., (n 15).

about fairness in criminal proceedings. The legal framework must address how to evaluate and mitigate these biases in AI-generated evidence. There is a need for legal safeguards to ensure that the use of AI does not infringe upon the rights of defendants or lead to unjust outcomes.<sup>54</sup> AI systems can inadvertently reflect biases present in the training data, leading to outcomes that disproportionately affect certain groups. This raises ethical concerns about fairness in legal proceedings. If AI evidence is shown to be biased, its use can undermine the integrity of the judicial process and lead to unjust outcomes.<sup>55</sup>

## CONCLUSION

The increasing use of artificial intelligence (AI) in various sectors, including law enforcement and judicial processes, presents both opportunities and challenges for the Tanzanian legal system. While AI-generated evidence could enhance the accuracy and efficiency of criminal investigations, it also raises complex issues concerning admissibility, relevance, and probative value within the Tanzanian framework of criminal law. Current Tanzanian statutes, such as the Evidence Act and the Electronic Transactions Act, provide foundational standards for evidence but do not specifically address the unique characteristics of AI-generated data, such as its opacity, potential biases, and technical complexities.

To incorporate AI evidence in a manner that upholds the principles of fairness and justice, Tanzanian courts must interpret existing laws in ways that acknowledge both the capabilities and the limitations of AI technologies. Additionally, there is a need for legislative reforms that explicitly regulate the use of AI in criminal proceedings, ensuring that AI-generated evidence meets established criteria of reliability, relevance, and transparency. Comparative insights from

other jurisdictions can offer valuable guidance in establishing standards that safeguard procedural rights and maintain the integrity of the justice system.<sup>56</sup>

Furthermore, theoretical frameworks like legal positivism and reliability theory underscore the importance of developing legal standards that align with technological advancements while remaining rooted in clear, socially accepted norms. As AI technology continues to evolve, Tanzanian courts and policymakers must proactively address its implications for evidence law, ensuring that AI serves as a tool for justice rather than a source of potential prejudice or error. This approach will help position Tanzania's legal system to effectively handle AI-related evidence, fostering a fair and accountable criminal justice system that is responsive to modern technological realities.

## Recommendations

To address the weaknesses associated with the use of AI-generated evidence in Tanzanian criminal proceedings, here are some targeted recommendations:

### Develop specific legislation for AI evidence

It is highly recommended that there is a huge need to introduce clear legislative provisions within the Evidence Act or as a standalone regulation that explicitly govern the use of AI-generated evidence. These provisions should define what constitutes AI evidence, establish criteria for admissibility, and set standards for assessing relevance and probative value.

### Establish reliability and transparency standards

Creating detailed guidelines for evaluating the reliability of AI algorithms and the data they generate. This could involve requiring AI

<sup>54</sup>Hunter, D., Mirko, B., and Nigel, S., "A framework for the efficient and Ethical use of Artificial Intelligence in Criminal Justice System", 47, Fla. St U. L 749, 2020, available at <<http://ir.law.fsu.edu/lr/vol47.iss4/7>>, (accessed on 8<sup>th</sup> October 2024).

<sup>55</sup> Sherman and Howard, "Addressing Challenges of Deepfakes and Artificial Intelligence Generated Evidence,

available at <<https://www.shermanhoward.com>> (accessed 27<sup>th</sup> October 2024).

<sup>56</sup> Artificial Intelligence Act, European Parliament, available at <<https://www.europarl.europa.eu>> (accessed 28<sup>th</sup> October 2024).

developers to disclose information about how algorithms function, including details on data sources, training methods, and any potential biases. These transparency requirements will help judges and legal practitioners understand the strengths and limitations of AI evidence.

### **Require independent expert testimony**

The law should put a clear mandate that AI-generated evidence shall be accompanied by expert testimony from certified, independent AI experts who can explain the processes behind the evidence. These experts can provide insight into the technology's accuracy and limitations in order to ensure the court has a well-rounded understanding of the evidence's reliability and probative value.

### **Establish a regulatory body for AI standards in evidence**

Due to the unique nature of AI there is a need to create a dedicated regulatory body to set and enforce standards for AI evidence, review new AI technologies, and maintain a registry of approved AI tools for use in criminal investigations and court proceedings. This body could provide certification for AI systems, ensuring only verified technologies are used within the justice system.

### **Training for judges and legal practitioners**

For experts to implement the unique nature of AI evidence there is a need to implement training programs for judges, prosecutors, and advocates on the technical and legal aspects of AI evidence. This will equip legal professionals with the knowledge to critically assess AI-generated data, evaluate its admissibility, and apply evidentiary standards consistently and fairly.

### **Adopt international best practices**

Draw on international practices and standards, such as those developed by the EU and the US, for managing AI evidence in courtrooms. Adopting best practices from these jurisdictions can provide Tanzanian lawmakers with a tested framework for

regulating AI in the justice system while adapting them to local needs.

### **Encourage public and scholarly discourse on AI in law**

Promoting academic and public discourse on the implications of AI evidence in criminal justice to create a well-rounded understanding of both its risks and benefits is most important at time. Public awareness and scholarly research can drive informed policy changes and help shape AI evidence laws that reflect social, ethical, and legal standards.

### **REFERENCES**

- Adejo, A. A., & Misau A.Y., "Application of Artificial Intelligence in Academic", 2021, available at <<https://www.researchgate.net>> (accessed 8 October 2024).
- Allen, *et al.*, Reforming the law of evidence of Tanzania (part two): conceptual overview and practical steps, 32(1), *Boston University International Law Journal*, 2013 pp. 1-53.
- Archak, D., "AI in Legal Evidence Analysis: Ethical and Legal Implications", 2(7), *International Journal for Legal Research and Analysis*, 2024, pp. 1-13.
- Art. 5(1) (a) the Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence, available at <<https://www.europarl.europa.eu>> (accessed 28th October 2024).
- Artificial Intelligence Act, European Parliament, available at <<https://www.europarl.europa.eu>> (accessed 28th October 2024).
- Bampasika, E., "Artificial Intelligence as Evidence in Criminal Trial", Doctoral Researcher, Member of the Otto Hahn Research Group on Alternative Criminal Justice Max Planck Institute for the Study of Crime, Security and Law Günterstalstraße 73, 79100, available at <[e.bampasika@csl.mpg.de](mailto:e.bampasika@csl.mpg.de)> , (accessed 4<sup>th</sup> October, 2024).
- Das, A., "Artificial Intelligence in Legal Evidence Analysis: Ethical and Legal Implications",

- 2(7), *International Journal for Legal research and Analysis*, 2024 pp. 1-13.
- Dory A.D., Reiling., "Courts and Artificial Intelligence", 11(2), *International Journal for Court Administration*, 2020, pp. 1-10.
- Dunsin, D., *et al*, "A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response", 2024, available at <<https://www.sciencedirect.com>>, (accessed 28<sup>th</sup> October 2024).
- Durán, J.M., van der Vloed, D., Ruifrok, A., & Ypma, R.J., "From understanding to justifying: computational reliabilism for AI-based forensic evidence evaluation", *Forensic Science International: Synergy*, 9, 2024, p.100554.
- Genty, E., "The Challenges of integrating AI-generated Evidence into the Legal system", 2024, available at <<https://www.akerman.com>> (accessed 17th August 2024).
- Gless, S., Lederer, I.F., and Weigend, T., "AI-Based Evidence in Criminal Trials?", 59, *Tulsa Law Review*, 2024, pp. 1-37.
- Grimm, P. W., *et al*, "Artificial Intelligence as Evidence" 19, *Northwestern Journal of Technology and Intellectual Property*, 2021, pp. 9-106.
- Handa, S and Thakur, S., "Role of AI in Admissibility of Electronic Evidence", 5(11), *International Journal of Research Publication and Reviews*, 2024, pp. 1323-8.
- Haider, R., Pearl, J., "AI-Driven Cyber Forensics: Investigating Cybercrimes and Strengthening Multi-Factor Authentication in E-Commerce" available at <<https://www.researchgate.net/publication>> (accessed 28th October, 2024).
- Hart, H., "*The Concept of Law*", (3rd edn), OUP, 2012.
- Hunter, D., Mirko, B., and Nigel, S., "A framework for the efficient and Ethical use of Artificial Intelligence in Criminal Justice System", 47, Fla. St U. L 749, 2020, available at <<http://ir.law.fsu.edu/lr/vol47.iss4/7/>>, (accessed on 8<sup>th</sup> October 2024).
- Jada, I., Mayayise, T.O., "The impact of artificial intelligence on organisational cybersecurity: An outcome of a systematic literature review" *Data and Information Management*, 2024 available at <[www.journals.elsevier.com/data-and-information-management](http://www.journals.elsevier.com/data-and-information-management)> (accessed 27th October 2024).
- Kapinga, A., "The Digital Transformation of Tanzania's Criminal Justice System; Opportunities and Challenges", 2024, available at < <https://papers.ssrn.com>> (accessed 12th July 2024).
- Lee, R., "The Inaccuracies of AI in Facial Recognition: Implications for Criminal Trials", 11, *Journal of Technology & Sociology*, 2020, pp. 23- 36.
- Ngowi, T., "Data Input and the Reliability of AI Systems in Criminal Forensics", 7, *African Digital Law Journal*, 2022, pp. 44-56.
- O'Neil, C., "*Weapons of Math Destruction*" , Crown, 2016.
- Orth, U., "Secondary victimization of crime victims by criminal proceedings", *Social justice research*, 15, 2002, pp. 313-25.
- Quezada, K., Vogiatzoglou, P., and Royer, S., "*Legal Challenges in Bringing AI Evidence to the Criminal Courtroom*", 2021, pp. 1-20.
- Rizwan, H., & Judea, P., "AI-Driven Cyber Forensics: Investigating Cybercrimes and Strengthening Multi-Factor Authentication in E-Commerce", available at <<https://www.researchgate.net/publication>> (accessed 28th October, 2024).
- Schindler, E., "Judicial system are turning to AI to help manage vast quantities of data and expedite case resolution", published on January, 8, 2024, accessed on 08, October 2024.



Sherman, H., “Addressing Challenges of Deepfakes and Artificial Intelligence Generated Evidence”, available at <<https://www.shermanhoward.com>> (accessed 27th October 2024).

Sushina, T., “Artificial Intelligent in criminal justice system; leading trends and possibilities, department of criminal procedure”, Kutafin Moscow State Law University, (MSAL), 4.

The National Prosecutions Service, “Criminal Prosecution Case Manual” 2023, available at <<https://tanzlii.org>>. (accessed 17th October 2024).

Unesco, How to determine the admissibility of AI generated evidence in Courts , 2023, available at <<https://www.unesco.org>> (accessed 7th October 2024).

Zafar, A., “Balancing the Scale: navigating ethical and practical challenges of AI integration in legal practice” 2024, available at <<https://link.springer.com>> (accessed 28th October 2024).

### **List of legislation**

Criminal Procedure Act [Cap 20 R.E 2022].

Evidence Act [Cap 6 R.E. 2022].

The Cybercrimes Act No 14 of 2015.

The Electronic Transaction Act, [Cap 442 R.E 2022].

The Penal Code [Cap 16 R.E 2022].

The Personal Data Protection Act [Cp 44 of 2022]