

	Global Journal of Arts Humanity and Social Sciences					
	ISSN: 2583-2034					
	Abbreviated key title: Glob.J.Arts.Humanit.Soc.Sci					
	Frequency: Monthly					
	Published By GSAR Publishers					
Journal Homepage Link: https://gsarpublishers.com/journal-gjahss-home/						
Volume - 6		Issue - 10		October 2026	Total pages 969-975	DOI: 10.5281/zenodo.23183733

LEGAL CHALLENGES AFFECTING THE APPLICATION OF ARTIFICIAL INTELLIGENCE WITHIN THE CRIMINAL JUSTICE SYSTEM IN TANZANIA

By

MPUNZA SARAFINA R

LL.M. Student at St. Augustine University of Tanzania, (SAUT).



Article History

Received: 25- 09- 2026

Accepted: 03- 10- 2026

Published: 06- 10- 2026

Corresponding author
**MPUNZA SARAFINA
R**

Abstract

The application of Artificial Intelligence (AI) in the criminal justice system offers opportunities to improve criminal investigations, evidence analysis, and the administration of justice. However, its use also raises significant legal challenges regarding right to a fair trial, privacy, and algorithmic bias, admissibility of evidence, transparency, and accountability. This article examines the legal challenges affecting the application of AI in Tanzania's criminal justice system. It analyzes the relevant constitutional and statutory framework and considers experiences from the United Kingdom, the European Union, India, and South Africa. The article argues that while existing laws in Tanzania provide some degree of protection, they do not comprehensively regulate AI. Consequently, it proposes specific legal and institutional reforms to ensure that AI is utilized in a manner that upholds fundamental rights and the rule of law.

Keywords: Artificial Intelligence, Criminal Justice, Data Protection, Right to a Fair Trial, Digital Evidence, Algorithmic Bias, Privacy.

1. INTRODUCTION

Artificial Intelligence has emerged as a significant technological development with the potential to transform the criminal justice system. AI technologies can assist law enforcement agencies in identifying suspects, analyzing vast amounts of data, handling digital evidence, performing facial recognition, and detecting patterns associated with criminal activity.ⁱ The use of these technologies can enhance efficiency and productivity in criminal investigations and judicial processes. However, the application of AI in the criminal justice system raises significant legal questions, given that criminal justice involves the exercise of state authority over individuals. So, decisions comes from the use of AI regarding surveillance, investigation, arrest, prosecution, and sentencing can directly impact an individual's liberty, privacy, dignity, and other fundamental rights.ⁱⁱ Consequently, the use of AI cannot be justified solely on the grounds that it is faster or more efficient than conventional methods, its application must adhere to principles of fairness, legality, accountability, due process, and equality.

In Tanzania, the legal challenges is substantial because there is no comprehensive legislation governing Artificial Intelligence.ⁱⁱⁱ Several existing laws relate to this issue, including the Constitution

of the United Republic of Tanzania 1977, the Criminal Procedure Act, the Evidence Act, the Cybercrimes Act, and the Personal Data Protection Act. However, these laws regulate specific aspects of criminal justice, digital information, and personal data rather than establishing an integrated legal framework for AI.^{iv} The central argument of this article is that Tanzania's existing legal framework provides a basis for regulating some consequences of AI but remains insufficient to address the various risks associated with algorithmic decision-making. In particular, existing laws do not adequately regulate AI-generated evidence, algorithmic bias, automated decision-making, explainability, accountability for AI-assisted decisions, or robust mechanisms to challenge such decisions.

Consequently, this article examines the key legal challenges affecting the application of AI within Tanzania's criminal justice system. It begins with the background of AI and criminal justice, followed by an examination of the relevant legal framework. It then analyzes the major legal challenges, considers comparative experiences from selected jurisdictions, and proposes recommendations to strengthen Tanzania's legal framework.



2. BACKGROUND TO THE APPLICATION OF ARTIFICIAL INTELLIGENCE IN CRIMINAL JUSTICE

Artificial Intelligence generally refers to technological systems capable of performing tasks associated with human intelligence, including learning, pattern recognition, classification, prediction, and decision support. Within the criminal justice system, AI can be utilized for predictive analysis, facial recognition, biometric identification, automated information processing, digital evidence analysis, and other investigative activities. The growing importance of AI stems partly from the rapid expansion of digital information. Criminal investigations may involve electronic communications, mobile phones, CCTV footage, electronic financial transactions, social media, and other forms of digital data. The volume of such information can exceed the capacity of investigators to analyze it manually. Artificial Intelligence can assist by processing vast amounts of data and identifying patterns or connections.^v

Thus, the use of AI can offer significant benefits to Tanzania. It can enhance the speed of investigations, assist in identifying relevant evidence, and aid law enforcement agencies in addressing increasingly complex forms of crime.^{vi} However, technological efficiency can also give rise to risks where AI systems produce inaccurate or discriminatory results. For instance, an inaccurate facial recognition system could lead to the misidentification of a suspect. Likewise, an algorithm trained on biased historical data could perpetuate discriminatory patterns in policing, where such outcomes influence decisions regarding arrests or prosecutions, technological errors can pose a direct threat to individual rights.^{vii} So, the legal significance of AI stems from its potential consequences rather than merely from the technology itself. When AI is employed by government institutions, its application must respect constitutional rights and established criminal justice principles.^{viii} This makes a robust legal framework essential to ensure that technological advancements do not undermine the rule of law.

3. LEGAL FRAMEWORK GOVERNING THE APPLICATION OF AI IN TANZANIA'S CRIMINAL JUSTICE SYSTEM

3.1 The Constitution of the United Republic of Tanzania, 1977

The Constitution serves as the primary legal foundation for regulating the use of AI within the criminal justice system. Article 13(1) states that all persons are equal before the law and are entitled to equal protection of the law, Article 13(6) provides essential procedural safeguards, including the right to a fair hearing and the presumption of innocence. These provisions have a direct impact on AI-assisted criminal justice. AI systems must not be designed or used in a manner that discriminates against individuals. Also, AI-generated assessments cannot replace the requirement that criminal liability be established through legally recognized

procedures and admissible evidence. Article 14 protects the right to life and personal liberty, while Article 15 safeguards personal freedom. These provisions are relevant where AI is used to identify suspects or support decisions leading to arrest or detention.^{ix} Therefore, algorithmic predictions should not, in isolation, serve as an independent legal basis for depriving a person of their liberty.

Also, Article 16 protects an individual's right to privacy and personal security. It specifically addresses facial recognition, biometric databases, surveillance, and the processing of personal data through AI systems. Article 30 further outlines limitations on the exercise of rights and freedoms, provided such restrictions are prescribed by law and are necessary for specific public interests and the rights of others. This strengthens the principle that intrusive AI applications must have a clear legal basis. Although the Constitution provides essential protections, it does not specifically regulate AI, therefore, constitutional safeguards require supplementation through comprehensive legislation and institutional frameworks.^x

3.2 Criminal Procedure Act, Cap. 20 R.E 2023

The Criminal Procedure Act, provides the primary legal framework governing criminal investigations and proceedings. It regulates matters such as arrests, searches, seizures, investigations, and criminal trials. This Act is pertinent to AI because law enforcement agencies may utilize AI to assist them in identifying suspects, analyzing information, or determining investigative priorities. However, the Act was enacted without specific regard for algorithmic decision-making. Consequently, it lacks detailed provisions concerning predictive analysis, automated suspect identification, algorithmic classification, or the use of AI-generated assessments in decisions affecting personal liberty.^{xi} Therefore, AI should remain an investigative tool that assists authorized officers, rather than serving as an independent source of legal authority for arrests, searches, or detentions.

3.3 Evidence Act, Cap. 6 R.E 2023

The Law of Evidence is significant because AI can be utilized in the processing, creation, verification, or interpretation of electronic information. Section 70 recognizes electronic evidence in criminal proceedings, while the admissibility of such evidence also intersects with requirements under the Electronic Transactions Act. This recognition of electronic evidence establishes a basis for using technology-derived information. However, AI-generated evidence raises issues that go beyond the mere existence of information in an electronic format. The court may need to decide whether the AI system is sufficiently reliable, whether the underlying data is accurate, and whether the methodology used to reach conclusions is scientifically and professionally sound. Consequently, while the existing legal framework provides a foundation for admitting electronic information, it does not fully address AI-derived conclusions, algorithmic reliability, error rates, training data, or explainability. This creates uncertainty when AI productions are trusted upon as evidence against an accused person.^{xii}

3.4 Cybercrimes Act, Cap. 443 R.E 2023

The Cybercrimes Act, provides a crucial framework for investigating and obtaining electronic information related to cybercrimes. Part IV of the Act regulates search and seizure, with sections 31 and 32 addressing the search, seizure, and disclosure of data. Sections 34 and 35 deal with the collection or disclosure of traffic and content data, while section 37 concerns forensic tools. These provisions can simplify the gaining and analysis of digital information that may later be processed using AI. Consequently, they are important to technology-assisted criminal investigations. However, the Act primarily regulates cybercrime and access to electronic information rather than AI itself. It does not comprehensively regulate automated decision-making, algorithmic classification, explainability, or liability for AI-generated conclusions, and discriminatory outcomes. Therefore, the power to collect electronic information should not be interpreted as an unlimited mandate to subject such information to any form of AI analysis.^{xiii}

3.5 Personal Data Protection Act, Cap. 44 R.E 2023

The Personal Data Protection Act, is highly significant as AI systems rely heavily on data. This law establishes a framework for the protection and processing of personal data and provides for institutional oversight through the Personal Data Protection Commission. The law is important to the criminal justice sector because AI technologies can process sensitive information, including biometric data, images, identification records, location data, and information linked to suspected criminal conduct. Consequently, the data protection framework offers essential safeguards against the unlawful processing of personal data. However, lawful processing does not guarantee that an AI system will yield accurate or non-discriminatory results. Therefore, data protection measures must be complemented by laws governing transparency, algorithmic fairness, human oversight, and accountability.^{xiv}

4. CURRENT LEGAL CHALLENGES AFFECTING THE APPLICATION OF AI IN TANZANIA'S CRIMINAL JUSTICE SYSTEM

4.1 Absence of Comprehensive AI Legislation

The greatest legal challenge is the absence of comprehensive legislation governing Artificial Intelligence. Existing laws regulate various aspects of technology, criminal procedure, electronic evidence, and personal data, but they do not provide a unified framework for AI. This creates uncertainty regarding which AI applications may legally be used by the police, prosecutors, and courts, what standards must be met prior to deployment, and what remedies should be offered to individuals affected by AI-assisted decisions.^{xv}

4.2 Privacy and AI-Based Surveillance

AI mostly enhances the capacity of public authorities to collect, aggregate, and analyze personal information. Biometric systems, automated surveillance and Facial recognition, can enable authorities to identify and track individuals to an extent that

conventional investigative methods could not easily achieve. Although Article 16 of the Constitution and the Personal Data Protection Act provide safeguards for privacy and personal information, AI raises further concerns because systems can combine disparate datasets to generate new information about individuals.^{xvi} Therefore, the law should establish clear limits regarding the collection and use of personal information through AI, especially where the technology is capable of continuous or large-scale monitoring.

4.3 Violation of the Right to a Fair Trial and Due Process

Article 13(6) (a) of the Constitution protects the right to a fair hearing. This right may be compromised when an accused person faces conclusions derived from AI without a meaningful opportunity to understand and challenge them. A person cannot effectively contest algorithmic outcomes if the government fails to provide sufficient information regarding the system, its reliability, and the basis upon which the results were generated. Thus, AI must not create an evidentiary environment where technical complexity prevents the accused person from exercising their right to a defence.^{xvii}

4.4 Violation of the Presumption of Innocence Principle

Algorithmic predictive and classification tools can create tension with the presumption of innocence principle. An AI system might classify an individual as having a high probability of criminal behavior based on historical or behavioral data. Such a prediction is not proof that the individual has committed a criminal offence. Consequently, the law must clearly distinguish between intelligence used to assist investigations and evidence capable of establishing criminal liability. AI predictions should not be treated as proof of guilt.^{xviii}

4.5 Algorithmic Bias and Equality before the Law

AI systems can perpetuate biases inherent in their training data. Where historical criminal justice data reflects discriminatory practices, an algorithm trained on such data may replicate or exacerbate those patterns. This raises direct concerns under Article 13(1) of the Constitution, which guarantees equality before the law.^{xix} Therefore, AI systems used by criminal justice institutions should undergo regular testing to determine if they produce discriminatory outcomes or not.

4.6 Lack of Transparency and Explainability

AI systems may employ complex algorithms that are difficult for laypeople, lawyers, and even judges to understand because it lack explainability how a certain conclusion was reached. This creates a legal issue where algorithmic outcomes affect individual rights. On the other hand, Transparency is crucial in criminal cases because decisions affecting liberty must be subject to legal scrutiny.^{xx} Consequently, the government should not rely on the technical complexity of an AI system to prevent an accused person from obtaining the information necessary to challenge an AI-supported conclusion.

4.7 Reliability of AI-Generated Evidence

The use of AI-generated or AI-assisted evidence raises questions regarding accuracy and reliability. An AI system may misidentify a person, misinterpret information, or produce incorrect predictions. Therefore, technological output should not automatically be accepted as proof of accuracy. Courts must have the capacity to examine the reliability and limitations of an AI system when its outputs are relied upon in criminal cases.^{xxi}

4.8 Accountability and Liability

Another challenge concerns accountability when AI contributes to an incorrect decision. For instance, if an AI system contributes to a misidentification or an unlawful investigative action, uncertainty may arise regarding whether liability lies with the police agency, an individual officer, or the technology provider. Such uncertainty should not prevent affected individuals from obtaining redress. The institution utilizing AI must retain legal responsibility for ensuring that the technology is lawful, adequately tested, and properly managed.^{xxii}

4.9 Limited Technical and Institutional Capacity

Effective AI governance requires technical knowledge among judges, prosecutors, police officers, lawyers, and regulatory authorities. Without sufficient expertise, criminal justice institutions might place undue reliance on AI outputs or fail to assess their reliability.^{xxiii} Therefore, capacity building is essential to ensure that AI is used responsibly and that courts can properly evaluate AI-assisted evidence.

5. COMPARATIVE EXPERIENCE FROM OTHER JURISDICTIONS

5.1 United Kingdom

The United Kingdom provides a significant example of regulating automated decision-making through data protection legislation. The Data Protection Act, 2018 includes safeguards regarding significant decisions based solely on automated processing. Sections 49 and 50 of the Act provide protections related to significant automated decisions within the context of law enforcement processing.^{xxiv} This framework was subsequently amended by the Data (Use and Access) Act, 2025. The revised approach permits certain automated decisions while maintaining safeguards, including notification to affected individuals, opportunities to make representations, human intervention, and the ability to challenge decisions. The UK approach demonstrates that AI need not be prohibited within the criminal justice system. Instead, high-impact applications may be permitted subject to meaningful human oversight and mechanisms for challenging decisions.^{xxv} So, on this context Tanzania could adopt a legal requirement that important AI-assisted decisions affecting criminal suspects must be subject to meaningful human review and an opportunity to challenge the decision.

5.2 European Union

The European Union has adopted a comprehensive regulatory approach through Regulation (EU) 2024/1689, known as the Artificial Intelligence Act. This legislation employs a risk-based approach wherein AI systems are regulated according to the level

of risk they pose to individuals and society. Article 5 of the Act regulates prohibited AI practices, including certain uses of biometric identification. The Act also imposes restrictions and safeguards on specific law enforcement applications and mandates stringent controls for high-risk AI systems. The EU framework is particularly relevant to criminal justice as it recognizes that AI applications affecting fundamental rights require stronger legal protections than low-risk applications.^{xxvi} Therefore, based on the EU legal framework governing AI, Tanzania could classify AI applications used for suspect identification, biometric surveillance, predictive policing, and other high-impact criminal justice functions as high-risk systems requiring prior assessment, human oversight, documentation, and independent monitoring.

5.3 India

India offers a valuable comparative example due to its rapid development of digital governance. The Digital Personal Data Protection Act, 2023, establishes a legal framework governing the processing of digital personal data. Section 4 stipulates that personal data may only be processed in accordance with the Act and for lawful purposes. The law also establishes obligations regarding notices, individual rights, and grievance redressed.^{xxvii} The Digital Personal Data Protection Rules, 2025, later provided further operational details for the data protection framework. Although India's framework focuses primarily on personal data rather than AI, it highlights the importance of establishing clear obligations for organizations that process digital information, as well as accessible mechanisms for individuals to lodge complaints.^{xxviii} So, the lesson for Tanzania is that, AI regulation should be closely linked to data protection legislation, given that AI systems rely heavily on personal and digital data. Tanzania should strengthen the mechanisms through which individuals can challenge the unlawful or risky processing of their information.

5.4 South Africa

South Africa offers a highly relevant African comparison. The Protection of Personal Information Act No. 4 of 2013 contains a specific provision addressing automated decision-making. Section 71 stipulates subject to specific exceptions, that a data subject shall not be subject to a decision resulting in legal consequences or significantly affecting them where that decision is based solely on automated processing intended to profile the individual. Where statutory exceptions apply, appropriate measures must be taken to safeguard the data subject's interests. These safeguards include the opportunity for the individual to make representations and access sufficient information regarding the underlying logic of the automated processing.^{xxix} Thus, on part of Tanzania, South Africa demonstrates the value of directly regulating automated decision-making within data protection legislation. Tanzania could similarly introduce provisions addressing AI-driven profiling and significant automated decisions, especially where such decisions affect autonomy or other fundamental rights.

6. RECOMMENDATIONS

6.1 Enacting Comprehensive AI Legislation



Tanzania should enact comprehensive legislation governing Artificial Intelligence, specifically addressing its application within the criminal justice system. The legislation should establish clear principles regarding fairness, transparency, legality, accountability, safety, human oversight, and the protection of fundamental rights. It should adopt a risk-based approach that distinguishes between low-risk and high-risk AI applications. Strict legal safeguards should apply to AI systems used in policing, surveillance, criminal investigations, biometric identification, evidence analysis risk assessment, and other activities that could significantly impact individual liberty or other fundamental rights. The legislation should also clearly define the legal responsibilities of government institutions, law enforcement agencies, technology service providers, and individual decision-makers when AI systems are utilized in the criminal justice context. This will address current legal uncertainty regarding liability when an AI system produces inaccurate, discriminatory, or unlawful outcomes.

6.2 Amending Criminal Procedure and Evidence Laws

The criminal procedure Act should be reviewed and amended to clarify the circumstances under which AI may be lawfully used during criminal investigations and trials. AI should function as a support tool for legally authorized officers and must not independently form the basis for arrest, search, detention, or prosecution. Any action affecting an individual's liberty must continue to rely on established legal procedures and the exercise of human judgment. On the other hand, the evidence Act should also be amended to establish specific rules governing AI-generated and AI-assisted evidence. Courts should be empowered to scrutinize the reliability, accuracy, methodology, data source, training process, potential bias, and limitations of an AI system whenever its output is relied upon as evidence. The law should also address the authenticity and chain of custody of digital evidence to ensure that the use of AI does not undermine the accused's right to a fair trial.

6.3 Strengthening Data Protection and Privacy

The Personal data protection Act should be strengthened to address challenges arising from biometric identification, AI profiling, predictive analysis, facial recognition, and the automated processing of personal information within the criminal justice system. Criminal justice institutions should be required to demonstrate that AI-based processing of personal information is lawful, necessary, proportionate, and linked to legitimate law enforcement purposes. Specific protections should apply to sensitive personal data and biometric information, where individuals should have access to mechanisms allowing them to challenge the unlawful or inaccurate processing of their personal information where appropriate.

6.4 Establishing Mandatory Human Oversight

Legislation should mandate meaningful and continuous human oversight regarding the use of high-risk AI applications within Tanzania's criminal justice system. AI must not independently determine criminal liability, guilt, sentencing, or punishment. Human decision-makers must retain genuine authority to review, reject, or modify AI-generated recommendations. Human oversight

should not be merely formal or perfunctory. Officials, prosecutors, and judicial officers involved in decisions involving AI must sufficiently understand the system's purpose, limitations, and potential risks to exercise independent judgment. This is particularly important where AI recommendations could influence decisions regarding arrest, bail, detention, prosecution, or sentencing.

6.5 Introduce Algorithmic Impact Assessments

Before high-risk AI systems are deployed within criminal justice institutions, mandatory algorithmic impact assessments must be conducted. These assessments should examine the system's accuracy, reliability, cybersecurity risks, privacy implications, and potential for bias, transparency, and possible impacts on constitutional and fundamental rights. The assessments should also consider whether the proposed AI system is necessary and proportionate to the objective for which it is being introduced. Where an assessment identifies unacceptable risks to individual rights, the system should not be deployed until appropriate safeguards are put in place.

6.6 Ensuring Transparency and Explainability of AI Systems

Criminal justice institutions should be required to maintain adequate documentation regarding the AI systems they employ. This should include information on the system's purpose, the type of data used, known limitations, accuracy rates, potential sources of bias, and the conditions under which its outputs can be relied upon. Where an AI-generated recommendation affects an individual's rights or liberty, the relevant authority should be able to provide an understandable explanation of the factors that contributed to the decision. The need for transparency must be balanced against legitimate concerns regarding national security, investigative techniques, and trade secrets, however, such concerns should not be used to completely preclude judicial scrutiny of artificial intelligence systems.

6.7 Establish Clear Rules Regarding Accountability and Liability

The law should establish clear rules determining accountability where AI contributes to an unlawful or harmful criminal justice decision. The use of AI must not create an accountability gap wherein government officials, institutions, and technology providers evade responsibility by attributing outcomes to the AI system. Law enforcement officers and other public officials should remain accountable for decisions made based on AI-generated information. At the same time, developers and technology providers should bear appropriate responsibility where negligence, defects, inadequate testing, or misrepresentations regarding their systems contribute to unlawful outcomes.

6.8 Strengthen Judicial Capacity and Oversight

Courts should be equipped with the necessary legal and technical capacity to scrutinize the use of AI in criminal cases. Judges and court officials should receive training on AI technologies, including their potential biases, evidentiary limitations, reliability, and impact on constitutional rights. Courts should have the

authority to require the disclosure of relevant information regarding the AI system when necessary to determine the admissibility or reliability of AI-assisted evidence. Judicial oversight is crucial in ensuring that technological efficiency does not take precedence over procedural fairness, legality, and the protection of fundamental rights.

6.9 Develop Institutional Guidelines and Code of Practice

Pending the enactment of comprehensive AI legislation, relevant criminal justice institutions should develop clear guidelines governing the procurement, deployment, and use of AI. Such guidelines should specify who may operate AI systems, the purposes for which they may be used, the types of decisions that may rely on AI outputs, record-keeping requirements, and procedures for reviewing erroneous results. These guidelines should complement, rather than replace legislation. Institutional policies like the National Artificial Intelligence Strategy 2025-2030 alone may not provide sufficient protection where AI usage infringes upon fundamental rights, therefore, legally enforceable safeguards should ultimately be established.

6.10 Fostering Responsible and Rights-Based AI Innovation

Ultimately, Tanzania should adopt a rights-based approach to the development and deployment of AI within the criminal justice system. AI has the potential to enhance the efficiency of investigations, evidence analysis, crime detection, and the administration of justice. However, technological efficiency should not be pursued at the expense of legality, human dignity, privacy, equality, due process, and the right to a fair trial. Therefore, the

government must ensure that the adoption of AI within the criminal justice system remains consistent with the Constitution, existing legal protections, and Tanzania's obligations under relevant international and regional human rights instruments. AI should function as a tool to support justice rather than replace legally accountable human decision-making.

7. CONCLUSION

The application of Artificial Intelligence within Tanzania's criminal justice system offers significant opportunities to improve criminal investigations and the administration of justice, but it also presents major legal challenges regarding fair trial, privacy, equality, algorithmic bias, the presumption of innocence, the reliability of evidence, and accountability. Although the Constitution, the Criminal Procedure Act, the Evidence Act, the Cybercrimes Act, and the Personal Data Protection Act provide important safeguards, they do not constitute a comprehensive legal framework for AI. Therefore, Tanzania should enact specific AI legislation, strengthen existing laws regarding criminal procedure and evidence, regulate high-risk AI applications, and mandate meaningful human oversight. Comparative experiences from the UK, the European Union, India, and South Africa demonstrate that AI can be integrated into the criminal justice system while effectively safeguarding fundamental rights. Finally, AI should remain a tool that assists legally authorized human decision-makers and must never serve as a substitute for constitutional guarantees, judicial accountability, and the rule of law.

END NOTES

ⁱ MARULI Sahat et al, (2024), *The Role of Artificial Intelligence in Criminal Justice*. Global International Journal of Innovative Research. P.1967-1978.

ⁱⁱ IWANNUDIN Irfan et al, (2025). *Legal challenges in regulating artificial intelligence use in criminal justice systems*. The Journal of Academic Science, Vol.2 No.6, P.1603-1611.

ⁱⁱⁱ RWETEMBURA Verus, (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), 1–18, p.136-146.

^{iv} The Constitution of the United Republic of Tanzania, 1977, Criminal Procedure Act Cap. 20 R.E 2023, Evidence Act Cap. 6 R.E 2023, Cybercrimes Act Cap. 443 R.E 2023 and Personal Data Protection Act Cap. 44 R.E 2023.

^v JOHN McCarthy, (2007), *what is Artificial Intelligence?* Stanford University; Human-Centered Artificial Intelligence. P. 2-3.

^{vi} MARULI Sahat et al, (2024), *The Role of Artificial Intelligence in Criminal Justice*. Global International Journal of Innovative Research. P.1967-1978.

^{vii} IWANNUDIN Irfan et al, (2025). *Legal challenges in regulating artificial intelligence use in criminal justice systems*. The Journal of Academic Science, Vol.2 No.6, P.1603-1611.

^{viii} UNESCO, (2021), *Recommendation on the Ethics of Artificial Intelligence*; Paris: United Nations Educational, Science and Cultural Organization.p.17- 43.

^{ix} The Constitution of the United Republic of Tanzania, 1977.

^x Ibid.

^{xi} Cap. 20 R.E 2023.

^{xii} Cap. 6 R.E 2023.

^{xiii} Cap. 443 R.E 2023.

^{xiv} Cap. 44 R.E 2023.

^{xv} RWETEMBURA Verus, (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), 1–18, p.136-146.



- ^{xvi} The Constitution of the United Republic of Tanzania, 1977.
- ^{xvii} Ibid.
- ^{xviii} Article 13 (6) (b) of the Constitution of the United Republic of Tanzania, 1977.
- ^{xix} The Constitution of the United Republic of Tanzania, 1977.
- ^{xx} IWANNUDIN Irfan et al, (2025). *Legal challenges in regulating artificial intelligence use in criminal justice systems*. The Journal of Academic Science, Vol.2 No.6, P.1603-1611.
- ^{xxi} RWETEMBURA Verus, (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), 1–18, p.136-146.
- ^{xxii} IWANNUDIN Irfan et al, (2025). *Legal challenges in regulating artificial intelligence use in criminal justice systems*. The Journal of Academic Science, Vol.2 No.6, P.1603-1611.
- ^{xxiii} Ibid.
- ^{xxiv} The Data Protection Act, 2018 (C. 12).
- ^{xxv} The Data (Use and Access) Act 2025 (C. 14).
- ^{xxvi} The European Union Artificial Intelligence Act, Regulation (EU) 2024/1689.
- ^{xxvii} The Digital Personal Data Protection Act, 2023 (N0.22).
- ^{xxviii} The Digital Personal Data Protection Rules, 2025.
- ^{xxix} The Protection of Personal Information Act No. 4, 2013 as amended 2022.