Article DOI: https://doi.org/10.37284/eajle.9.1.4515



East African Journal of Law and Ethics
eajle.eanso.org
Volume 9, Issue 1, 2026
Print ISSN: 2707-532X| Online ISSN: 2707-5338
Title DOI: https://doi.org/10.37284/2707-5338



Original Article

Cybercrime and Jurisdiction in Tanzania: A Central Challenge to Law Enforcement Authorities

Mathan Laiseck Chalamila

[1] The Open University of Tanzania, P. O. Box 19, Ludewa, Tanzania.
[*] Author for Correspondence Email: chalamila2013@gmail.com

Article DOI: https://doi.org/10.37284/eajle.9.1.4515

Date Published:

16 February 2026

Keywords:

Cybercrime, Jurisdiction, Cyberspace, Sovereignty.

ABSTRACT

The borderless nature of cyberspace poses significant challenges to the exercise of criminal jurisdiction by states. Before the advancement of technology principle governing criminal jurisdiction was basically tied to the geographical area. In Tanzania, the prosecution of cybercrime raises complex questions concerning prescriptive, adjudicative, and enforcement jurisdiction, particularly where offences are committed wholly or partly outside national territory. This article critically examines the jurisdictional framework governing cybercrime prosecution in Tanzania, with specific reference to the Cybercrimes Act, [Cap 443, R.E 2023]. It analyses the extent to which Tanzanian courts and law enforcement authorities are legally empowered to investigate, prosecute, and adjudicate cybercrime offences with cross-border elements. Drawing on comparative jurisprudence and relevant international legal instruments, this article evaluates the adequacy of Tanzania's statutory framework in addressing jurisdictional challenges in cyberspace. It argues that while Tanzanian law provides a foundational basis for asserting jurisdiction over cybercrime, doctrinal ambiguities, enforcement limitations, and dependence on international cooperation significantly constrain its effectiveness. As stated, cybercrimes are committed over the internet, which may involve various persons from different countries. The issue of jurisdiction, as to whether law enforcement officers have the power to arrest and prosecute for an offence committed out of their jurisdiction, has to be determined first.

APA CITATION

Chalamila, M. L. (2026). Cybercrime and Jurisdiction in Tanzania: A Central Challenge to Law Enforcement Authorities. *9*(1), 185-191. https://doi.org/10.37284/eajle.9.1.4515

CHICAGO CITATION

Chalamila, Mathan Laiseck. 2026. "Cybercrime and Jurisdiction in Tanzania: A Central Challenge to Law Enforcement Authorities" *East African Journal of Abdulswamad Haji Sunnaf Law and Ethics* 9 (1), 185-191. https://doi.org/10.37284/eajle.9.1.4515

HARVARD CITATION

Chalamila, M. L. (2026) "Cybercrime and Jurisdiction in Tanzania: A Central Challenge to Law Enforcement Authorities" *East African Journal of Law and Ethics*, 9(1), pp. 185-191. doi: 10.37284/eajle.9.1.4515.

IEEE CITATION

M. L. Chalamila. "Cybercrime and Jurisdiction in Tanzania: A Central Challenge to Law Enforcement Authorities", *EAJLE*, vol. 9, no. 1, pp. 185-191, Feb. 2026.

 This work is licensed under a Creative Commons Attribution 4.0 International License.

Article DOI: https://doi.org/10.37284/eajle.9.1.4515

MLA CITATION
Chalamila, Mathan Laiseck. "Cybercrime and Jurisdiction in Tanzania: A Central Challenge to Law Enforcement Authorities" *East African Journal of Law and Ethics*, Vol. 9, no. 1, Feb. 2026, pp. 185-191, doi:10.37284/eajle.9.1.4515.

INTRODUCTION

The rapid expansion of information and communication technologies has transformed the manner in which criminal activities are committed, investigated, and prosecuted. Unlike traditional crimes, the power to control activities conducted through cyberspace is challenging[1]. Cybercrimes are frequently committed across national borders, often without the physical presence of the offender in the territory where the harm is experienced[2]. This characteristic of cyberspace presents profound challenges to classical principles of criminal jurisdiction, which are traditionally grounded in territorial sovereignty[3].

In Tanzania, the enactment of the Cybercrimes Act, 2015, marked a significant legislative response to offences committed through computer systems and information and communication technologies. However, the application of this framework to cybercrime prosecutions raises complex jurisdictional questions, particularly where offences involve foreign perpetrators, victims located in multiple states, or data stored outside national territory[4]. Determining whether Tanzanian courts and law enforcement authorities possess lawful competence to prescribe, adjudicate, and enforce criminal liability in such circumstances remains a central challenge.

Despite the growing importance of jurisdiction in cybercrime enforcement, much of the existing discourse has focused on defining cybercrime and categorising its various forms[5]. While such discussions provide useful background, they do not adequately address the core legal difficulty posed by cyberspace: the erosion of clear territorial boundaries upon which criminal jurisdiction is traditionally exercised[6]. For courts and prosecutors, the principal challenge lies not in identifying cyber offences, but in establishing lawful jurisdiction over conduct that transcends national borders[7].

This article, therefore, focuses specifically on jurisdiction as a legal and institutional challenge in the prosecution of cybercrime in Tanzania. It examines how Tanzanian law conceptualises and applies prescriptive, adjudicative, and enforcement jurisdiction in relation to cyber offences and assesses whether the existing statutory framework adequately responds to the realities of cross-border cybercrime. The analysis is situated within a comparative and international legal context, drawing on selected foreign jurisprudence and international legal instruments governing cybercrime and jurisdiction.

METHODOLOGY

This article adopts a doctrinal legal research methodology, complemented by a comparative analytical approach. The doctrinal method is employed to examine the legal framework governing cybercrime jurisdiction in Tanzania, with particular focus on the Cybercrimes Act[8] and related legislation. Primary legal sources, including statutes, judicial decisions, and international legal instruments, constitute the core materials for analysis. International and Regional legal instruments establish procedural powers and facilitate cooperation among states in investigating and prosecuting cyber offences. The Budapest Convention on Cybercrime[9] has

[1] Hemlata Sharma and Kiran Mishra, Jurisdiction Issues in Cybercrimes: A challenging Approach, *Ideal Journal of Management &IT*, .X, 51 (August, 2019), ISSN 2277-8489.

[2] Santha, F. Problems of Jurisdiction in Cybercrimes Cases, University of Miskolc, Doi: 1032041/978836714976 at page 133.

[3] Janine Kremling and Amanda M. Sharp Parker, *Cyberspace, Cybersecurity and Cybercrime*, SAGE Publication Inc., (2018), 85

[4] Msengi, Ismail Emmanuel. "The Role of Law Enforcement in Combating Financial Cybercrimes in Tanzania: Examining the Laws and Practice", *East African Journal of Law and Ethics*, 7, (1), 205, https//doi.org/10.37284/eajle.7.1.2497.

[5] Ellen S.Podgor, "Cybercrime: National, Transnational or International?" *50 Wayne L. Rev.97* (2004), 97.

[6] Ibid.

[7] Ellen, "Cybercrime: National, Transnational or International?", 98

[8] [Cap443, R.E.2023]

[9] 2001

 This work is licensed under a Creative Commons Attribution 4.0 International License.

Article DOI: https://doi.org/10.37284/eajle.9.1.4515

influenced domestic legislation like the Tanzania Cybercrime Act[10] , which contains many of the categories of cyber offences and procedural powers found in the Convention. The African Union Convention on Cyber Security and Personal Data Protection is a regional legal instrument which provide framework for African countries' cooperation and legal approach in respect to jurisdiction, which can facilitate cross-border investigation.

Judicial decisions from Tanzanian courts are analysed to assess how jurisdictional provisions are interpreted and applied in practice, particularly in cases involving cross-border elements. This examination is supplemented by selected foreign jurisprudence, which is used comparatively to illuminate alternative approaches to jurisdiction in cyberspace and to evaluate the consistency of Tanzanian law with emerging international norms.

The study also engages with relevant scholarly literature on cybercrime, jurisdiction, and international criminal law to contextualise the doctrinal analysis and identify prevailing theoretical and practical challenges. The methodology is qualitative in nature and does not rely on empirical data collection. Rather, it seeks to provide a critical legal evaluation of jurisdictional competence and limitations through systematic interpretation of legal texts and judicial reasoning.

LEGAL FRAMEWORK GOVERNING CYBERCRIME IN TANZANIA

a) The Cybercrime Act[11]

Cybercrime in Tanzania is primarily regulated by the Cybercrimes Act, which criminalises a range of offences relating to computer systems, electronic communications, and data. The Act provides substantive offences, investigative powers, and procedural mechanisms intended to facilitate the prosecution of cybercrime[12].

While the Act establishes a statutory basis for addressing cyber offences, its effectiveness depends largely on how jurisdictional provisions are framed and applied. Cybercrime prosecutions often involve conduct that is initiated outside Tanzania, infrastructure located abroad, or victims dispersed across multiple jurisdictions. These realities place significant strain on domestic legal frameworks that were traditionally designed for territorially bounded crimes.

b) Electronic Postal and Communication Act (EPOCA)[13]

Although the law does not specifically cover cybercrime issues, it is a vital law for the regulatory regime for electronic and communication service providers. The law establishes a national response team to deal with all incidents relating to cybersecurity[14]. Any person who uses network facilities or network services fraudulently commits an offence and, once convicted, is liable to a fine of Tanzania shilling five million or imprisonment for a term of not more than two years or both penalties[15].

c) The Electronic Transaction Act[16]

This law recognises any transaction conducted electronically, the use of information and communication technologies, as well as the admissibility of electronic evidence. The Act also provides for the use of a secured electronic signature in the execution of various electronic documents, which aims at identifying culprits' fraudulent persons who may likely occur in endorsing the signature in the electronic document[17]. In identifying the electronic signature, the law sets out two conditions to be met[18]: -

[10] Ibid.

[11] Ibid

[12] Ibid. Part IV sections 31-35.

[13] [Cap 306, R.E 2023]

[14] Ibid section 124(1)

[15] Ibid section 122(b)

[16] [Cap 442, R.E 2023]

[17] Ibid section 6

[18] Ibid

 This work is licensed under a Creative Commons Attribution 4.0 International License.

Article DOI: https://doi.org/10.37284/eajle.9.1.4515

- The method is used to identify the person and to indicate the intention of that person in relation to information communicated; and
- At the time the method was used, that method was reliable and appropriate for the purposes for which the information was communicated

JURISDICTIONAL CHALLENGES IN THE PROSECUTION OF CYBERCRIME

Prescriptive Jurisdiction

Prescriptive jurisdiction refers to a state's authority to enact laws regulating particular conduct. In the context of cybercrime, this authority is complicated by the borderless nature of cyberspace, where harmful conduct may originate outside national territory but produce effects within it.

Jurisdiction determines which court has the authority to hear a matter and to determine the sentence for a crime. In traditional criminal law, the principle is based mainly on territorial jurisdiction within the locality of the given state[19]. The Cybercrimes Act[20] extends jurisdiction to offences committed wholly or partly within Tanzania, offences involving computer systems or data located within the country, and offences committed by Tanzanian nationals abroad. These provisions reflect recognised principles of international law, including territoriality, nationality, and the effects doctrine. However, the Act does not clearly articulate the thresholds for asserting extraterritorial jurisdiction, particularly where neither the offender nor the relevant infrastructure is physically located in Tanzania. This poses a challenge where cybercrime is not recognised as an extradition offence, and the accused person, who is located in a foreign country, commits an offence against a victim in Tanzania.

This lack of precision creates uncertainty for prosecutors and courts and risks inconsistent application of the law. Clear statutory articulation of the circumstances under which extraterritorial conduct falls within Tanzanian jurisdiction is essential to ensure legal certainty and compliance with international law. The requirement set out in the Council of Europe's Convention on Cybercrime (Budapest) is that the offence has to be punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State[21].

Enforcement Jurisdiction

Enforcement jurisdiction refers to a state's authority to investigate, arrest, and enforce criminal law. International law strictly limits the exercise of enforcement powers within the territory of another state without consent. In cybercrime investigations, these limitations are particularly acute[22]. Discrepancies in national laws in criminal laws create a challenge in handling cybercrimes, unlike in traditional criminal jurisdiction. The effectiveness of extra-territorial jurisdiction and extradition law has been found to be challenging because of internet fragmentation and the contradictions of national laws in regulating criminal machinery[23]. While Tanzanian law enforcement authorities possess extensive investigative powers within the national territory, these powers cannot lawfully be exercised extraterritorially. Where suspects or digital evidence are located abroad, authorities must rely on international cooperation mechanisms, which are often slow and procedurally complex[24]. Enforcement jurisdiction for cases emanating within Tanzania, where the accused person and the computer system used in

[19] Jun Li and Jidong Jia, "Confusion and Relief of Criminal Jurisdiction of Cybercrimes", *Advances in Computer Science Research*, 65, Atlantis Press, (2018) 51, http://creativecommons.org/licenses/by-nc/4.0/

[20] Ibid note 8 section 30

[21] Article 22(1)(d) of the Budapest Convention

[22] Mohamed Tarek Hasan, "Cross-Border Cybercrimes and International Law: Challenges in ensuring justice in a digitally connected world", *Journal of Law and Cybercrime,* 4, (1) (November, 2024), 3.

[23] Phenyo Sekati, "Assessing the effectiveness of Extradition and the Enforcement of Extra-Territorial Jurisdiction in Addressing Trans-national Cybercrimes", *Comparative and International Law Journal of South Africa*, 55, (1) (2022), 1, https://doi.org/10.25159/2522-3062/10476.

[24] Alfred, Stephano, "Jurisdictional challenges in prosecuting the publication of false information under Tanzania's Cybercrime Act: The Problem of Extra-territorial offences", *International Journal for Multidisciplinary Research*, 7, (6) (November-December,2025), 2.

 This work is licensed under a Creative Commons Attribution 4.0 International License.

Article DOI: https://doi.org/10.37284/eajle.9.1.4515

committing the offence are located within the United Republic of Tanzania, enforcement authorities have been successfully handling such cases[25]. The challenge comes when the accused person and the computer system is located out of the country, but the victim is within the United Republic of Tanzania. There is no great challenge for Tanzanian courts on the jurisdictional issue if the crime is committed by an accused who resides within the country[26]. The challenge comes when the offence is committed by an accused person who resides in a foreign country, and there is no enhanced collaboration between the two countries. Establishing a standardised binding treaty for data sharing will enhance in combating cybercriminals[27].

International and Comparative Perspectives

International legal instruments, most notably the Budapest Convention on Cybercrime, of which Tanzania is not a signatory, provide guidance on jurisdictional principles and cooperation mechanisms[28]. Comparative analysis demonstrates that clearer statutory provisions and stronger cooperation frameworks enhance states' ability to address cross-border cybercrime[29]. States have the freedom to apply theories of jurisdiction and the duty to take action where the offence is committed within their territorial jurisdiction[30]. Applying the principles stated by the Budapest Convention becomes easy for finding the solution to jurisdictional issues relating to cybercrimes, so long as state cooperation is enhanced and dual criminality is applied. A landmark *Yahoo case*[31] which has created jurisdictional conflict for matters concerning cyberspace. Yahoo, which operated a website hosted in the USA, allowed, through auction, the sale of *Nazi memorabilia*, the items which contained Nazi symbols, which were legal under USA laws but were strictly prohibited under French laws. The French NGOs sued Yahoo in a French court for violation of French criminal law by allowing French citizens to view and purchase Nazi items. The court ruled that French courts had jurisdiction to determine the matter based on where the harmful effects occurred, without regard to where the servers are located[32]. Under the Cybercrime Act, Tanzania criminalizes publication of prohibited or misleading information, the use of a computer system to commit unlawful acts, as well as online content that violates Tanzanian law.[33] The Internet is all about information, and information carries the whole issue of freedom of speech, which is a constitutional right recognised by every state. So whether the providing state is responsible for defining freedom of speech or the recipient country, the question raises challenges for cybercrime enforcement authorities when it comes to combating cyber offences[34].

Enforcement of Cybercrime Jurisdiction in Tanzania

The enforcement of cybercrime jurisdiction depends on institutional capacity, statutory powers, and effective international cooperation. In Tanzania, cybercrime enforcement is primarily undertaken by the Police Force, in collaboration with the Office of the Director of Public Prosecutions and relevant regulatory authorities. Section 3 of the Cybercrime Act define law enforcement officer to mean[35];

> *...a police officer of the rank of Assistant Inspector or above, or an investigator of equivalent rank of inspector and above, member of Tanzania Intelligence Service, prosecutor or any authorised officer of the authority responsible for the regulation of*

[25] Livinus Kidamabi @Tengwa v Republic, Criminal Appeal No.96 of 2022 (HC-Shinyanga) (unreported)

[26] Ibid

[27] Ibid note 20, page 6.

[28] Jacopo Bratta, "Jurisdiction issues in cybercrimes", *Law and Media working Paper Series,* No.4/2021 at page 4.

[29] Ibid.

[30] Ibid.

[31] Yahoo Inc v LICRA (2000)

[32] Mathias Reimann, "Introduction: The Yahoo! Case and Conflict of Laws in the Cyberage", 24(3), *Mich. J. Int'l L.* 663 (2003), 666, https://repository.law.umich.edu/mjil/vol24/iss3/1.

[33] Section 16

[34] Ibid page 667.

[35] [Cap 443, R.E.2023]

 This work is licensed under a Creative Commons Attribution 4.0 International License.

Article DOI: https://doi.org/10.37284/eajle.9.1.4515

communication or any other person authorised in any written law…

The Cybercrimes Act confers powers of search, seizure, preservation, and access to computer data[36]. However, these powers are territorially limited and ineffective where evidence or suspects are located abroad. As a result, enforcement relies heavily on mutual legal assistance and extradition, mechanisms that are often inadequate for the speed and complexity of cybercrime investigations[37].

Given the legal processes of extradition and mutual assistance through which countries assist each other in criminal matters, countries are faced with the dual criminality principle, where the offence which is committed must be a crime in the other requested state[38]. Most of the social media in Tanzania are *Instagram, Facebook, X* (formerly *Twitter*), *TikTok,* etc., which are domiciled in the US and Europe[39]. They are not bound by the Tanzanian law, and the only way of conducting criminal machinery is through Mutual Legal Assistance and extradition, which often is delayed or rejected due to the reasons of non-existence of international agreement, absence of dual criminality, issues of a discriminatory nature[40] , etc.

The absence of detailed procedural standards tailored to cyber investigations further undermines enforcement effectiveness and increases the risk of evidentiary challenges in court. Emerging international debates on direct access to data and cooperation with internet intermediaries highlight potential avenues for reform, but also raise significant legal concerns where issues may be rejected for reasons reserved for the country itself as a basis of jurisdiction[41].

CONCLUSION

Cybercrime poses fundamental challenges to traditional principles of criminal jurisdiction. In Tanzania, the Cybercrimes Act, 2015 provides a necessary foundation for regulating cyber offences, but its effectiveness is constrained by doctrinal ambiguities, enforcement limitations, and reliance on international cooperation mechanisms.

For Tanzania to effectively prosecute cybercrime in a manner consistent with international law, greater clarity in jurisdictional provisions, enhanced institutional capacity, and stronger engagement with international legal frameworks are required. Addressing these challenges is essential to ensuring that jurisdiction asserted under domestic law can be meaningfully enforced in the digital age.

Recommendations

International cooperation has to be enhanced through bilateral and multilateral agreements on cybercrime enforcement. The scope and thresholds of extraterritorial jurisdiction have to be clearly clarified in the Cybercrime Act. Capacity building in specialized on cybercrime and digital evidence has to be strengthened for judicial and prosecutors.

REFERENCES

Conventions

Council of Europe's Convention on Cybercrime (Budapest Convention) 2001.

African Union Convention on Cyber security and Personal Data Protection, 2020

Statutes

Cybercrime Act [Cap 443, R.E 2023]

[36] Ibid. Part IV of the Act, section 31

[37] TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATION 54 (Michael N. Schmitt, ed. 2nd edn.2017).

[38] Alex Marwa Mwita, "Mutual Legal Assistance and Extradition as Tools for International Cooperation in Tanzania: Practice and Challenges", *East African Journal of Law and Ethics*, 8, (1) (2025), 353, Doi: https://doi.org/10.37284/eajle.8.1.3652.

[39] Ibid note 22.

[40] Guideline to Prosecutors and Competent Authorities for Making and Executing Mutual Legal Assistance and Extradition Request win Tanzania, May 2023.

[41] Eli Scher-Zagier, "Jurisdiction Creep: The UN Cybercrime Convention and the Expansion of Passive Personality Jurisdiction", *Yale Journal of Law &Technology,* 27, (1) (2025), 359.

 This work is licensed under a Creative Commons Attribution 4.0 International License.

Article DOI: https://doi.org/10.37284/eajle.9.1.4515

Electronic Postal and Communication Act (EPOCA) [Cap 306, R.E 2023]

The Electronic Transaction Act [Cap 442, R.E 2023]

Guidelines

Guideline to Prosecutors and Competent Authorities for Making and Executing Mutual Legal Assistance and Extradition Request in Tanzania, May 2023.

Text Books

Janine Kremling and Amanda M. Sharp Parker, *Cyberspace, Cybersecurity and Cybercrime*, SAGE Publications Inc., (2018).

TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATION 54 (Michael N. Schmitt, ed. 2nd edn. 2017).

Journals

Alex Marwa Mwita, "Mutual Legal Assistance and Extradition as Tools for International Cooperation in Tanzania: Practice and Challenges", *East African Journal of Law and Ethics*, 8, (1) (2025), Doi: https://doi.org/10.37284/eajle.8.1.3652 (344-355)

Alfred, Stephano, "Jurisdictional challenges in prosecuting the publication of false information under Tanzania's Cybercrime Act: The Problem of Extra-territorial offences", *International Journal for Multidisciplinary Research*, 7, (6) (November-December, 2025), pp1-5.

Eli Scher-Zagier, "Jurisdiction Creep: The UN Cybercrime Convention and the Expansion of Passive Personality Jurisdiction", *Yale Journal of Law &Technology,* 27, (1) (2025), 359.

Ellen S. Podgor, "Cybercrime: National, Transnational or International?" *50 Wayne L. Rev.97* (2004)

Hemlata Sharma and Kiran Mishra, Jurisdiction Issues in Cybercrimes: A Challenging Approach, *Ideal Journal of Management &IT*, X, 51 (August, 2019)

Jacopo Bratta, "Jurisdiction issues in cybercrimes", *Law and Media Working Paper Series,* No.4/2021

Jun Li and Jidong Jia, "Confusion and Relief of Criminal Jurisdiction of Cybercrimes", *Advances in Computer Science Research*, 65, Atlantis Press, (2018), http://creativecommons.org/licenses/by-nc/4.0/

Mathias Reimann, "Introduction: The Yahoo! Case and Conflict of Laws in the Cyberage", 24(3), *Mich. J. Int'l L.* 663 (2003), 666, https://repository.law.umich.edu/mjil/vol24/iss3/1.

Mohamed Tarek Hasan, "Cross-Border Cybercrimes and International Law: Challenges in ensuring justice in a digitally connected world", *Journal of Law and Cybercrime,* 4, (1) (November, 2024)

Msengi, Ismail Emmanuel. "The Role of Law Enforcement in Combating Financial Cybercrimes in Tanzania: Examining the Laws and Practice", *East African Journal of Law and Ethics*, 7, (1), 205, https//doi.org/10.37284/eajle.7.1.2497.

Phenyo Sekati, "Assessing the effectiveness of Extradition and the Enforcement of Extra-Territorial Jurisdiction in Addressing Trans-national Cybercrimes", *Comparative and International Law Journal of South Africa*, 55, (1) (2022), 1 36, https://doi.org/10.25159/2522-3062/10476.

Santha, F. Problems of Jurisdiction in Cybercrimes Cases, University of Miskolc, Doi: 1032041/

Case Laws

Livinus Kidamabi @Tengwa v Republic, Criminal Appeal No.96 of 2022 (HC-Shinyanga) (unreported).

Yahoo Inc v LICRA (2000)

 This work is licensed under a Creative Commons Attribution 4.0 International License.