

Jurisdictional Challenges in Prosecuting the Publication of False Information under Tanzania's Cybercrimes Act: The Problem of Extraterritorial Offences

Alfred Stephano

Candidate LLM ICT LAW, Public and Private Law, University of Iringa

Abstract

The digital era has intensified the transnational spread of false information, creating significant challenges for national legal systems. In Tanzania, section 16 of the Cybercrimes Act, 2015 criminalizes the intentional publication of false or misleading information, while section 4 asserts jurisdiction over extraterritorial offences. Despite these provisions, prosecutions remain limited, particularly where the alleged conduct originates abroad. This article examines the jurisdictional, constitutional, institutional, and international cooperation challenges undermining enforcement of section 16. Drawing on Tanzanian case law, international instruments such as the Budapest and Malabo Conventions, and comparative jurisprudence, the article argues that the current framework inadequately balances state interests with freedom of expression. It concludes that legislative reform, institutional strengthening, and enhanced international cooperation are essential to ensure Tanzania's cybercrime regime is both effective and rights-compliant.

Keywords: Cybercrime; False Information; Extraterritorial Jurisdiction; Tanzania; Freedom of Expression; Digital Forensics.

1. Introduction

The rapid expansion of internet communication has enabled unprecedented access to information but has equally facilitated the global circulation of misinformation and disinformation. Governments have responded by criminalizing the publication of false information in efforts to safeguard public order, national security, and democratic integrity. In Tanzania, the Cybercrimes Act, 2015 represents a key legislative response. Section 16 prohibits the publication of "false, deceptive, misleading or inaccurate information," while section 4 extends jurisdiction extraterritorially to conduct committed abroad that produces substantial effects within the country.¹

Despite these provisions, practical enforcement has proved elusive. When false information originates outside Tanzania, prosecutions are undermined by principles of state sovereignty, the requirement of dual criminality, reliance on Foreign Service providers for digital evidence, and weak domestic institutional

¹ *Cybercrimes Act, 2015* (Tanzania), ss 4, 16.

capacity. Furthermore, the breadth of section 16 raises constitutional concerns, as it risks encroaching upon the guarantee of freedom of expression under Article 18 of the Constitution.²

This article addresses the question: **What are the jurisdictional challenges in prosecuting the publication of false information under Tanzania's Cybercrimes Act when the offence is committed extraterritorially?** The analysis proceeds in five parts: Part 2 examines the domestic legal and constitutional framework; Part 3 analyses jurisdictional and international cooperation challenges; Part 4 explores institutional and evidentiary barriers; Part 5 considers the balance between free expression and criminalization; and Part 6 offers recommendations for reform.

2. Legal and Constitutional Framework

Section 16 of the Cybercrimes Act, 2015 criminalizes the intentional publication of false information through computer systems.³ Section 4 extends this provision beyond Tanzania, covering offences committed abroad with substantial effects in the country. While consistent with international law principles such as the effects doctrine, enforcement abroad requires cooperation with foreign states.

Article 18 of the Constitution guarantees freedom of opinion, expression, communication, and access to information. These rights are limited under Article 30, which permits restrictions for national security, public order, and morality.⁴

Japhet Ibrahim Matarra v Republic, the appellant posted tweets alleging that the President had improperly accumulated wealth. The High Court (Moshi) upheld his conviction under section 16, holding that failure to prove the truth of the allegations established falsity and intent to mislead.

The judgment effectively shifted the burden of proof to the accused, undermining the presumption of innocence under Article 13(6) (a) of the Constitution and Article 14(2) of the ICCPR.⁵

In addition, provisions in the Media Services Act criminalize false news publications and defamation,⁶ creating duplication with section 16. The Evidence Act further complicates matters, as it itself does not contain clear procedures for admitting electronic evidence, leaving courts to rely on general rules ill-suited for digital forensics.⁷

3. Jurisdictional and International Cooperation Challenges

Section 4 of the Cybercrimes Act asserts extraterritorial jurisdiction, aligning with the effects principle. However, as established in the *Lotus Case*, the ability to prescribe jurisdiction is distinct from the ability to enforce it.⁸ Tanzania cannot unilaterally enforce its laws abroad without foreign cooperation.

The principle of dual criminality, embedded in the Extradition Act and Mutual Assistance in Criminal Matters Act, requires that conduct be criminalized in both Tanzania and the requested state.⁹ Since many jurisdictions treat false information as civil defamation or protected expression, Tanzania struggles to extradite suspects or secure evidence.

² *Constitution of the United Republic of Tanzania, 1977*, art 18, art 30.

³ *Ibid*, s 16.

⁴ *Ibid*, art 30.

⁵ *Japhet Ibrahim Matarra v Republic*, Criminal Appeal No 51 of 2023 (HC Moshi).

⁶ *Media Services Act*, Cap 229 [R.E. 2023], ss 36–54.

⁷ A Mollel and Z Lukumay, *Electronic Transactions and Law of Evidence in Tanzania* (Iringa University College 2007) 64.

⁸ *The Lotus Case (France v Turkey)* [1927] PCIJ Rep Series A No 10.

⁹ *Extradition Act*, Cap 368 R.E. 2019, s 4; *Mutual Assistance in Criminal Matters Act*, Cap 254 R.E. 2022.

Tanzania is not a party to the Budapest Convention on Cybercrime (2001),¹⁰ nor has it ratified the African Union Malabo Convention (2014).¹¹ As a result, Tanzania lacks access to expedited cross-border data preservation, mutual assistance mechanisms, and harmonized offence definitions, isolating its enforcement efforts.

4. Institutional and Practical Barriers

Tanzania faces significant institutional barriers to prosecuting cybercrimes offences:

The Cybercrime Unit lacks sufficient digital forensic expertise, accredited laboratories, and advanced investigative tools.¹² Prosecutors and magistrates often lack training in handling electronic evidence, leading to weak or inconsistent rulings.

Livinus Kidamabi @ Tengwa v Republic The appellant was convicted for unauthorized access to electronic data under cybercrime provisions. On appeal, he argued the evidence was unreliable. The High Court (Shinyanga) quashed the conviction, finding that the prosecution failed to establish a proper chain of custody for the electronic evidence.

The case underscores how poor handling of digital evidence undermines cybercrime prosecutions in Tanzania.¹³

Tanzania is also heavily dependent on Foreign Service providers such as Google, Meta, and X (Twitter) for crucial evidence. These companies, domiciled in the US and EU, are not bound by Tanzanian law and respond only through formal MLA requests, which are often delayed or rejected due to the absence of bilateral treaties.¹⁴

5. Balancing Free Expression and Criminalization of False Information

The broad scope of section 16 risks criminalizing legitimate speech, satire, and political criticism, raising concerns under Article 19 of the ICCPR and Article 18 of the Tanzanian Constitution. International jurisprudence emphasizes that restrictions on expression must be lawful, necessary, and proportionate.¹⁵

Salov v Ukraine (ECtHR, 2005) A newspaper editor was convicted for publishing allegedly false information during Ukraine's presidential election. The European Court of Human Rights ruled the conviction violated Article 10 of the ECHR, as the sanction was disproportionate and unnecessary in a democratic society.

This case highlights the international reluctance to criminalize false information broadly. Tanzania's section 16 risks similar disproportionate outcomes, undermining constitutional and human rights guarantees.¹⁶

6. Recommendations

Reforming Tanzania's cybercrime framework requires legislative, institutional, international, and policy interventions to ensure effectiveness while safeguarding fundamental rights. Section 16 of the

¹⁰ Council of Europe, *Convention on Cybercrime* (Budapest, 2001).

¹¹ African Union, *Malabo Convention on Cybersecurity and Personal Data Protection* (2014).

¹² AJ Mambi, *Information and Communication Technologies and Cyber Law* (Mkuki na Nyota 2010) 115.

¹³ *Livinus Kidamabi @ Tengwa v Republic*, Criminal Appeal No 96 of 2022 (HC Shinyanga).

¹⁴ EW Lubua, 'Cybercrimes Incidents in Financial Institutions of Tanzania' (2014) 14 IJCSBI 1.

¹⁵ ICCPR, art 19(3); African Commission on Human and Peoples' Rights, *Declaration of Principles on Freedom of Expression in Africa* (2002).

¹⁶ *Salov v Ukraine* (2005) ECHR 65518/01.

Cybercrimes Act 2015 should be amended to target harmful misinformation, such as fraud, incitement to violence, or threats to public health, rather than criminalizing all “false” content.¹⁷ Clear definitions and thresholds for liability will protect freedom of expression, consistent with the Constitution of the United Republic of Tanzania 1977, art 30, and ICCPR, art 19(3).¹⁸ The Evidence Act should be updated to include procedures for digital evidence, covering collection, authentication, and admissibility of electronic records and social media communications.¹⁹ Harmonization with the Media Services Act, Section 36–54, and the Electronic Transactions Act will create a coherent legal framework for cybercrime prosecution.²⁰

Institutional strengthening is critical to effective enforcement. Establishing an accredited digital forensic laboratory will allow reliable analysis of computers, mobile devices, servers, and cloud platforms, while ISO-accreditation ensures international credibility.²¹ Prosecutors, magistrates, and judges should receive specialized training on emerging technologies, digital evidence, and balancing enforcement with human rights.²² A dedicated cybercrime unit within the Director of Public Prosecutions’ office would centralize expertise, coordinate investigations, and develop prosecutorial guidelines for complex cases.²³

International cooperation should be enhanced through ratification of the Council of Europe, Convention on Cybercrime (Budapest, 2001) and the African Union, Malabo Convention on Cyber security and Personal Data Protection (2014), providing harmonized frameworks and 24/7 points of contact.²⁴ Bilateral treaties with countries hosting major service providers will facilitate evidence preservation and cross-border investigations.²⁵ Such measures ensure Tanzania can respond effectively to transnational cyber offences and collaborate internationally to prosecute offenders.²⁶

Policy measures should focus on prevention and public engagement. Nationwide digital literacy campaigns can educate citizens about recognizing harmful content, practicing safe online behavior, and reporting cybercrime incidents.²⁷ Co-regulation with digital platforms under TCRA oversight will promote efficient content moderation while protecting human rights.²⁸ Civil remedies, such as retractions and corrections, should be prioritized before criminal sanctions, reserving prosecution for repeated or high-risk conduct.²⁹ These strategies balance freedom of expression with public safety and reduce pressure on the courts.

In combination, these interventions legislative, institutional, international, and policy will create a resilient cybercrime framework in Tanzania. Precision in legal definitions, capacity-building, cross-border cooperation, and preventive measures will strengthen enforcement while safeguarding fundamental rights.

7. Conclusion

Tanzania’s Cybercrimes Act 2015 represents a significant legislative step toward addressing online offe-

¹⁷ Cybercrimes Act 2015 (Tanzania), s 16.

¹⁸ Constitution of the United Republic of Tanzania 1977, Article 30; ICCPR, Article 19(3).

¹⁹ A Mollé and Z Lukumay, *Electronic Transactions and Law of Evidence in Tanzania* (Iringa University College 2007) 64.

²⁰ Media Services Act, Cap 229 [R.E. 2023], Section 36–54.

²¹ EW Lubua, ‘Cybercrimes Incidents in Financial Institutions of Tanzania’ (2014) 14 *IJCSBI* 1.

²² AJ Mambi, *Information and Communication Technologies and Cyber Law* (Mkuki na Nyota 2010) 115.

²³ *Japhet Ibrahim Matarra v Republic*, Criminal Appeal No 51 of 2023 (HC Moshi).

²⁴ Council of Europe, *Convention on Cybercrime* (Budapest, 2001); African Union, *Malabo Convention on Cybersecurity and Personal Data Protection* (2014).

²⁵ Extradition Act, Cap 368 [R.E. 2019], Section 4; Mutual Assistance in Criminal Matters Act, Cap 254 [R.E. 2022].

²⁶ UNODC, *Comprehensive Study on Cybercrime* (United Nations Office on Drugs and Crime, 2013) 125.

²⁷ EW Lubua, ‘Cybercrimes Incidents in Financial Institutions of Tanzania’ (2014) 14 *IJCSBI* 1.

²⁸ Cybercrimes Act of 2015, Section 16.

²⁹ Constitution of the United Republic of Tanzania 1977, Article 30.

nces. However, the offence of publishing false information continues to raise constitutional concerns, face jurisdictional challenges, and suffer from institutional weaknesses, compounded by reliance on Foreign Service providers that may be uncooperative. Without comprehensive reforms legislative, institutional, and international enforcing Section 16 effectively will remain difficult. A balanced approach is essential, one that targets harmful misinformation while protecting fundamental freedoms and upholding the rule of law. Strengthening legal clarity, institutional capacity, and international cooperation is therefore critical for a resilient and rights-respecting cybercrime framework in Tanzania.

BIBLIOGRAPHY

Books and Monographs

1. AJ Mambi, *Information and Communication Technologies and Cyber Law* (Mkuki na Nyota 2010) 115.
2. D Bainbridge, *Introduction to Computer Law* (5th edn, Pearson 2004) 201.
3. A Mollel and Z Lukumay, *Electronic Transactions and Law of Evidence in Tanzania* (Iringa University College 2007) 64.

Statutes

1. Constitution of the United Republic of Tanzania 1977, arts 18, 30.
2. Cybercrimes Act 2015, Section 4, 16.
3. Evidence Act Cap 6 R.E 2023 Section 44, 86
4. Extradition Act, Cap 368 [R.E. 2023], Section 4,
5. Mutual Assistance in Criminal Matters Act, Cap 254[R.E. 2022].
6. Media Services Act, Cap 229[R.E. 2023], Section 36–54.

Cases

1. Japhet Ibrahim Matarra v Republic, Criminal Appeal No 51 of 2023 (HC Moshi).
2. Livinus Kidamabi @ Tengwa v Republic, Criminal Appeal No 96 of 2022 (HC Shinyanga).
3. The Lotus Case (France v Turkey) [1927] PCIJ Rep Series A No 10.
4. Salov v Ukraine (2005) ECHR 65518/01.

International Instruments and Declarations

1. African Commission on Human and Peoples' Rights, Declaration of Principles on Freedom of Expression in Africa (2002).
2. African Union, Malabo Convention on Cyber security and Personal Data Protection (2014).
3. Council of Europe, Convention on Cybercrime (Budapest, 2001).
4. International Covenant on Civil and Political Rights 1966, art 19(3).
5. UNODC, Comprehensive Study on Cybercrime (2013) 125.

Journal Articles

1. EW Lubua, 'Cybercrimes Incidents in Financial Institutions of Tanzania' (2014) 14 IJCSBI 1.