Page 3305 - 3313 **DOI:** *https://doi.org/10.63108/IJLMH.13083*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 5

2026

© 2026 *International Journal of Law Management & Humanities*

Follow this and additional works at: https://www.ijlmh.com/
Under the aegis of VidhiAagaz – Inking Your Brain (https://www.vidhiaagaz.com/)

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of **any suggestions or complaints**, kindly contact **support@vidhiaagaz.com**.

To submit your Manuscript for Publication in the **International Journal of Law Management & Humanities**, kindly email your Manuscript to **submission@ijlmh.com.**

The Effectiveness of the Tanzania Police Force in Preventing and Protecting Against Cyber Mobile Bullying in Tanzania

JOVIN DIDACE*

ABSTRACT

The widespread use of smartphones and digital communication platforms has intensified concerns about cyber mobile bullying in Tanzania. This article critically examines the effectiveness of the Tanzania Police Force in preventing such conduct and protecting victims, with particular attention to statutory authority, investigative capacity and constitutional safeguards. Using a purely doctrinal methodology, it analyses the Constitution of the United Republic of Tanzania, the Cybercrimes Act, the Electronic Transactions Act, the Police Force and Auxiliary Services Act, relevant judicial decisions and international cybercrime instruments. The analysis finds that existing laws provide mechanisms to investigate some forms of online harassment, but their dispersed provisions do not offer a comprehensive, victim-centred response to cyber mobile bullying. Investigations also face potential obstacles relating to digital evidence, technical expertise, anonymity, underreporting and cross-border cooperation. Since the study relies on documentary sources rather than police operational data or interviews, it evaluates the legal and institutional conditions of effectiveness rather than measuring actual case-resolution rates. It argues for clearer statutory standards, stronger digital forensic capacity, accessible reporting and victim-support mechanisms, rights-compliant investigations, and sustained public education. An integrated approach is essential to effective protection without unjustifiably restricting privacy and freedom of expression.

Keywords: *cyber mobile bullying, Tanzania Police Force, cybercrime, victim protection, digital evidence*

I. INTRODUCTION

Digital communication has brought substantial benefits to social interaction, commerce and access to information. Yet mobile devices and online platforms also enable persistent intimidation, threatening messages, humiliation, dissemination of private material and other forms of technology-facilitated abuse.

* Author is an LL.M. Student at University of Iringa, Iringa, Tanzania.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

Conduct of this kind can follow victims beyond schools, workplaces and homes, while anonymous accounts and the rapid circulation of content complicate identification and intervention. Scholarly studies distinguish cyberbullying from conventional face-to-face bullying through features including technological mediation, persistence, audience reach and the difficulty of escaping harmful content.[1]

In Tanzania, the central legal question is not whether the Police Force possesses authority to respond to harmful online conduct. The relevant issue is whether the combination of criminal prohibitions, evidentiary powers, institutional resources and protective procedures provides an intelligible and effective response to cyber mobile bullying.

The Police Force is legally mandated to preserve the peace, prevent and detect crime and apprehend offenders, while the Cybercrimes Act establishes offences and investigative mechanisms applicable to unlawful conduct committed through computer systems and information and communication technologies.[2] The exercise of these powers must nevertheless be consistent with constitutional guarantees relating to equality, dignity, privacy, personal security and the protection of individual rights.[3]

This article argues that legal authorisation is necessary but insufficient for effective policing of cyber mobile bullying. Police responsiveness depends upon clearly identified offences, lawful access to reliable electronic evidence, practical investigative capacity, accessible complaint mechanisms and coordinated victim protection. The admissibility and reliability of electronic evidence are particularly important because cyberbullying investigations commonly depend upon electronic messages, social-media communications, digital records and other electronically generated information.[4] Moreover, enforcement effectiveness cannot be measured solely by arrests or prosecutions. Prevention, prompt intervention, victim protection and respect for constitutional safeguards are equally important components of an effective legal response.

II. Background to the Problem

The growth of mobile phones, social media and instant messaging has improved communication but has also facilitated harassment, intimidation, humiliation and other forms of harmful online

[1] *See* Robin M. Kowalski, Susan P. Limber & Patricia W. Agatston, Cyberbullying: Bullying in the Digital Age (2d ed. 2012); Peter K. Smith et al., *Cyberbullying: Its Nature and Impact in Secondary School Pupils*, 49 J. Child Psych. & Psychiatry 376, 376–85 (2008), https://doi.org/10.1111/j.1469-7610.2007.01846.x.
[2] Police Force and Auxiliary Services Act, Cap. 322, § 5(1) (R.E. 2023) (Tanz.); Cybercrimes Act, Cap. 443, pts. II, IV (R.E. 2023) (Tanz.).
[3] Tanz. Const. arts. 12, 13, 15, 16 (1977).
[4] Electronic Transactions Act, Cap. 442, § 18 (R.E. 2023) (Tanz.); Cybercrimes Act pt. IV.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

conduct. Cyberbullying differs from traditional bullying because harmful content may spread rapidly, reach large audiences, remain accessible for long periods and follow victims beyond physical spaces.[5]

For this article, cyber mobile bullying refers to intentional or sustained harmful conduct carried out through mobile devices or digital platforms. The term is used analytically and is not itself a statutory expression, although section 23 of the Cybercrimes Act creates an offence of cyber bullying. Particular acts may fall within that or other existing offences, depending on their nature and circumstances.[6]

Tanzania regulates cyber-related misconduct mainly through the Cybercrimes Act, the Electronic Transactions Act, the Criminal Procedure Act and the Police Force and Auxiliary Services Act.[7] Electronic evidence is particularly important in cyberbullying cases, and its reliability, integrity and origin must be properly established.[8] Enforcement must also respect constitutional rights, including dignity, privacy, personal security and freedom of expression.

International instruments such as the Budapest Convention, the Malabo Convention and the United Nations Convention against Cybercrime provide comparative guidance on cybercrime investigation, electronic evidence and international cooperation.[9] The central concern, therefore, is whether Tanzania's existing legal and institutional framework enables the Police Force to investigate and respond effectively to cyber mobile bullying while protecting constitutional and procedural rights. This article evaluates that question doctrinally; it does not claim to quantify actual police performance, which would require empirical data.

III. Legal and Institutional Challenges

A. Uncertainty in the legal treatment of cyber mobile bullying

Section 23 of the Cybercrimes Act expressly establishes the offence of cyber bullying. Section 23(1) prohibits a person from initiating or sending an electronic communication using a computer system to another person with intent to coerce, intimidate, harass or cause emotional distress. Under section 23(2), contravention attracts, on conviction, a fine of not less than five

[5] Sameer Hinduja & Justin W. Patchin, Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying (2d ed. 2015); Robert S. Tokunaga, *Following You Home from School: A Critical Review and Synthesis of Research on Cyberbullying Victimization*, 26 Computers Hum. Behav. 277 (2010), https://doi.org/10.1016/j.chb.2009.11.014.

[6] Cybercrimes Act §§ 15, 16, 23.

[7] Cybercrimes Act; Electronic Transactions Act; Criminal Procedure Act, Cap. 20 (R.E. 2023) (Tanz.); Police Force and Auxiliary Services Act.

[8] Electronic Transactions Act § 18(2).

[9] Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185 (entered into force July 1, 2004); African Union Convention on Cyber Security and Personal Data Protection, June 27, 2014; United Nations Convention against Cybercrime, G.A. Res. 79/243, annex (Dec. 24, 2024).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

million shillings, imprisonment for a term of not less than three years, or both. Consequently, the legal issue is not the absence of an offence, but whether its language and the available procedures address the diverse forms of cyber mobile bullying.[10]

Section 23(1) specifies an intended harmful purpose but does not expressly require repeated communications or proof that emotional distress actually occurred. Its operative words, however, focus on initiating or sending an electronic communication to another person. It is therefore necessary to examine, case by case, whether public posts about an individual, coordinated harassment, impersonation or other platform-based abuse satisfy these elements or fall under another offence, particularly section 15 (impersonation by means of a computer system) or section 16 (publication of information known to be false, deceptive, misleading or inaccurate) of the Act. The existence of criminal punishment under section 23(2) also does not itself establish a comprehensive framework of immediate protective orders, counselling, reporting assistance or victim-specific remedies. These are possible remedial gaps requiring further analysis, not proof that cyberbullying is unregulated. Investigative measures remain subject to the distinct conditions in sections 31–38.[11]

B. Institutional capacity and responsiveness

Section 5(1)(a)–(d) of the Police Force and Auxiliary Services Act assigns the Force the duties of preserving the peace, maintaining law and order, preventing and detecting crime, and apprehending and guarding offenders. For individual officers, section 27(3)(c)–(e) prescribes the prevention of offences, the detection of offenders and their lawful apprehension. Cyberbullying investigations additionally depend on the specialised powers in sections 31–38 of the Cybercrimes Act. These provisions establish legal authority but do not themselves show that victims can report easily, that digital evidence is preserved promptly or that specialist support is available. Those matters require independent assessment.[12]

Scholarly literature identifies difficulties associated with cyberbullying and digital evidence, including pseudonymous identities, persistent or deleted online content and cross-border platforms. The statutory provisions for preservation and data disclosure respond to some of these problems, but do not establish the adequacy of training, equipment or institutional coordination in the Tanzania Police Force. Without interviews, operational records or case-outcome data, this doctrinal article cannot conclude that particular police units lack capacity,

[10] Cybercrimes Act § 23(1)–(2).
[11] *Id.* §§ 15, 16, 23(1)–(2), 31–38.
[12] Police Force and Auxiliary Services Act §§ 5(1)(a)–(d), 27(3)(c)–(e); Cybercrimes Act §§ 31–38.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

nor can it quantify response failures. Instead, it identifies the resources and procedures that would need empirical evaluation.[13]

C. Preservation of electronic evidence and cross-border investigation

Electronic evidence is particularly vulnerable to deletion, alteration and loss. Cyberbullying complaints may involve disappearing messages, renamed accounts and devices with limited storage capacity. Prompt preservation, forensic handling and proper documentation are therefore essential to maintain the integrity and admissibility of digital evidence.[14] Police should also distinguish immediate victim-protection measures from later evidential steps, so that urgent protection is not unnecessarily delayed until the full criminal investigation is complete.[15]

Where online platforms or service providers are located outside Tanzania, investigations may raise additional issues concerning jurisdiction, subscriber information, attribution and international legal assistance. Delays in obtaining data and differences between national legal systems may weaken investigations. Effective enforcement therefore requires coordination among the Police Force, prosecutors, communication regulators, service providers and authorised foreign counterparts, alongside clear domestic investigative powers.[16]

D. Underreporting and access to victim protection

Reluctance to report cyberbullying may arise from embarrassment, fear of retaliation, limited awareness and concern about confidentiality,[17] although the present doctrinal study does not measure the prevalence of such barriers in Tanzania. The duty to prevent and detect offences arises under sections 5(1)(c) and 27(3)(c)–(d) of the Police Force and Auxiliary Services Act. The applicable investigative powers are more specific: section 31(1) of the Cybercrimes Act concerns authorised search and seizure on the required reasonable grounds; section 32(1)–(3) concerns disclosure of data and applications for court orders; section 33(1) concerns expedited preservation where data is vulnerable to loss or modification; sections 34 and 35 regulate traffic and content data; and sections 36–38 prescribe the associated court-order, forensic-tool and application-hearing procedures. These provisions cannot be treated as an unrestricted power to access private communications or as an express entitlement to counselling.[18]

---

[13] *See* KOWALSKI ET AL., *supra* note 1; Tokunaga, *supra* note 5.
[14] Electronic Transactions Act § 18(2); Cybercrimes Act §§ 33, 37(4)–(5).
[15] *See* Police Force and Auxiliary Services Act; Criminal Procedure Act.
[16] Cybercrimes Act pt. IV; Criminal Procedure Act; United Nations Convention against Cybercrime, *supra* note 9.
[17] *See* UNITED NATIONS CHILDREN'S FUND, *Cyberbullying: What Is It and How to Stop It* (last updated Jan. 2026), https://www.unicef.org/end-violence/how-to-stop-cyberbullying (questions 2, 5–6) (last visited Oct. 24, 2026).
[18] Police Force and Auxiliary Services Act §§ 5(1)(c), 27(3)(c)–(d); Cybercrimes Act §§ 31(1), 32(1)–(3), 33(1), 34–38.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

Accordingly, victim protection should combine accessible reporting instructions, child-sensitive and confidential handling, prompt risk assessment and suitable referrals. Information given to complainants should explain how to preserve original digital communications and how conduct may be reported under section 23 of the Cybercrimes Act. Any police request for information or interference with devices must comply with the applicable statutory conditions and article 16 of the Constitution, while article 18 makes it necessary to distinguish prohibited intimidation or harassment from lawful expression. More detailed victim-support arrangements are recommendations for reform, not powers presumed from the Police Force's general mandate.[19]

E. Constitutional protection of privacy and expression

The Constitution of the United Republic of Tanzania protects privacy and freedom of expression. Article 16 safeguards personal privacy and private communications, while article 18 protects freedom of opinion, expression and communication.[20] These rights are relevant to cyber mobile bullying because harmful disclosure of private communications may interfere with privacy, while enforcement against online content must avoid unjustified restrictions on lawful expression.

The State must therefore balance victim protection with constitutional safeguards. Police investigations should address genuine threats and harassment without resorting to indiscriminate surveillance, unjustified access to communications or criminalisation of protected expression. In *Jamii Media Company Limited v. Attorney General*, the High Court dismissed a constitutional petition, brought principally on privacy grounds, against the data-disclosure power in section 32 of the Cybercrimes Act and the ex parte, in camera hearing of applications under section 38, and upheld both provisions. As reported, the court held that disclosure requests under section 32 were not arbitrary and that the provision struck a proportionate balance between individual rights and the public interest.[21]

Accordingly, cybercrime laws should contain clear offences, defined investigative powers and proportionate safeguards. This promotes legal certainty while protecting both victims of online abuse and constitutional rights. Necessity and proportionality provide additional safeguards. A legitimate protective objective does not justify every means of achieving it. Investigators and

[19] Cybercrimes Act §§ 23, 31–38; TANZ. CONST. arts. 16, 18.
[20] TANZ. CONST. arts. 16, 18.
[21] *Jamii Media Co. v. Attorney General*, Misc. Civil Cause No. 9 of 2016 (H.C. Tanz. Main Registry 2017), *as reported in* Ashnah Kalemera, *Tanzania Court Deals a Blow to Intermediary Liability Rules*, CIPESA (Apr. 26, 2017), https://cipesa.org/2017/04/tanzania-court-deals-a-blow-to-intermediary-liability-rules/; *Tanzania: Cybercrimes Act Upheld in Further Blow to Free Expression*, ARTICLE 19 (Mar. 15, 2017), https://www.article19.org/resources/tanzania-cybercrimes-act-upheld-in-further-blow-to-free-expression/ (reporting that the High Court declared sections 32 and 38 constitutional); *see also* TANZ. CONST. arts. 16, 18; Cybercrimes Act §§ 32, 38.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

courts should examine the gravity and context of alleged conduct, the risks to victims, available evidence and the intrusiveness of proposed measures. Measures affecting confidential communications should be specifically authorised, properly supervised and limited to what the applicable law permits.

These considerations are especially important when harmful conduct occurs in a dispute that also contains political commentary, investigative journalism, personal criticism or public-interest speech. The law must distinguish genuine threats, targeted harassment and other prohibited conduct from communication that remains constitutionally protected. Protection of victims and fidelity to constitutional rights should be viewed as mutually reinforcing features of legitimate policing.

F. International cooperation and legal safeguards

Cybercrime investigations often require international cooperation where offenders, electronic data or platform operators are located outside Tanzania. The Budapest Convention, the Malabo Convention and the United Nations Convention against Cybercrime provide useful comparative standards on electronic evidence, preservation of data, mutual assistance and cross-border cooperation.[22] Their relevance, however, depends on Tanzania's treaty status and applicable domestic law.

Tanzania signed the United Nations Convention against Cybercrime on 25 October 2025, but the Convention had not entered into force as at October 2026.[23] It therefore remains important for domestic investigators to rely on lawful national procedures while making precise and timely requests for preservation of electronic data, subscriber information and other evidence held abroad.

IV. Recommendations

A. Clarify the scope of section 23 and strengthen victim remedies

Reform should commence with section 23 of the Cybercrimes Act, which already criminalises electronic communications intended to coerce, intimidate, harass or cause emotional distress. A focused review should assess how subsection (1) applies to persistent messaging, public posts about victims, coordinated attacks and impersonation, including possible overlap with sections

[22] Convention on Cybercrime, *supra* note 9; African Union Convention on Cyber Security and Personal Data Protection, *supra* note 9; United Nations Convention against Cybercrime, *supra* note 9.

[23] *United Nations Convention against Cybercrime*, United Nations Treaty Collection, https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-16&chapter=18 (status as at Oct. 24, 2026: United Republic of Tanzania signed Oct. 25, 2025; not yet in force) (last visited Oct. 24, 2026); United Nations Convention against Cybercrime, *supra* note 9, art. 65(1).

15 and 16. If practical or doctrinal gaps are demonstrated, clarification should be narrowly framed and should avoid criminalising constitutionally protected expression. Consideration should also be given to accessible reporting, timely preservation under section 33, proportionate protective relief and referrals to victim-support services, subject to procedural safeguards and articles 16 and 18 of the Constitution.[24]

B. Strengthen specialist police training and digital forensic capacity

Specialist cybercrime training should include mobile-device evidence, preservation of platform data, lawful identification of account holders, forensic documentation, victim interviewing and the presentation of electronic records in court. Police units should have access to appropriate technical expertise and standardised protocols, with supervisory review of investigative requests that affect privacy. Resource allocation should be informed by evidence of case volume, complexity and outcomes rather than by assumption alone.

C. Improve reporting channels and victim protection

Accessible complaint channels should accommodate reports made online or at ordinary police stations and should offer clear guidance on urgent threats, preservation of original messages and available follow-up procedures. Privacy and safeguarding arrangements are particularly necessary for children and for people facing intimate-image abuse or repeated intimidation. Police cooperation with schools, regulators, welfare services and civil society may strengthen referral pathways while preserving confidentiality.

D. Enhance cooperation and institutional accountability

Formal procedures for working with domestic service providers and foreign counterparts should clarify the legal basis, scope and record-keeping of data requests. Publicly available, appropriately aggregated information about complaint handling and case outcomes would also enable more rigorous assessment of police performance without exposing victims' identities. Research involving victims, investigators and prosecutors is necessary to test the practical operation of the framework described in this article.

E. Promote constitutional and procedural safeguards

Guidelines on digital searches, preservation demands and online-content investigations should require legality, necessity, proportionality, careful documentation and judicial oversight where required. Legitimate expression must be distinguished from unlawful threats and harassment.

[24] Cybercrimes Act §§ 15, 16, 23, 33; TANZ. CONST. arts. 16, 18.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

F. Strengthen public education and preventive engagement

Police and relevant agencies should develop public guidance on reporting abusive communications, maintaining original electronic records, obtaining urgent support and using available complaints procedures. Schools, parents, civil society organisations and communications providers can support targeted prevention initiatives.

V. CONCLUSION

Tanzania has statutory and institutional mechanisms capable of responding to several forms of harmful communication conducted through mobile devices. However, a general police mandate and dispersed cybercrime provisions cannot alone establish an effective system for preventing and protecting against cyber mobile bullying. The doctrinal analysis identifies the need for more precise legal standards, stronger evidence-handling capacity, easier reporting, better coordinated victim support and reliable cross-border cooperation. Such measures must be designed with the constitutional rights to privacy, expression and fair process firmly in view. The strongest approach is therefore integrated and rights-based: one that combines proportionate enforcement with prevention, technical competence and demonstrable accountability. Because the study is doctrinal, empirical assessment of police practices and victim outcomes remains an important next step.

*****

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]