Akungba Communication and Media Journal
Vol. 2, No. 2, October 2025: 1-17 ISSN: 1115–621X

TANZANIA'S CYBERCRIMES ACT: A STAKEHOLDER ANALYSIS OF ITS IMPACT ON FREEDOM OF EXPRESSION

Tabu Manyama

Department of Mass Communication
School of Communication Studies,
St. Augustine University of Tanzania
manyama@saut.ac.tz

Abstract

This study critically investigated stakeholders' views on sections of Tanzania's Cybercrimes Act No. 14 of 2015 that infringe on freedom of expression. To guide its argument, the study was underpinned by the Chilling Effect Theory, which posits that vague laws can lead individuals to self-censor to avoid potential punishment. The key informant interview method was employed, involving 22 respondents selected through purposive sampling. Data were collected via unstructured interviews. The selected respondents include media practitioners from the Tanzania Editors' Forum, representatives from TWAWEZA, a civil society organisation focused on freedom of expression and policy analysis, academicians teaching Journalism and Mass Communication at St. Augustine University of Tanzania, Media Council of Tanzania, the Tanzania Human Rights Defenders Coalition, and the Legal and Human Rights Centre. Major findings revealed that several sections of the Cybercrimes Act directly infringe upon freedom of expression in Tanzania, for example, sections 16, 20 and 31, to mention a few. Also, the findings identified that the Act imposes overly broad content restrictions, penalises undefined terms such as "false information," enables excessive surveillance without proper judicial oversight, and allows arbitrary enforcement with harsh penalties. This environment fosters significant self-censorship and reporting restrictions among journalists. It is concluded that an urgent re-evaluation and reform of the Cybercrimes Act are imperative to align it with fundamental freedoms and ensure a balanced digital legal framework. It is recommended, among others, that the Act introduce explicit legal protections for journalists and their sources, prioritise investment in technical cybersecurity infrastructure over punitive measures, and shift from a one-size-fits-all approach to a Customised Approach.

Keywords*:* Freedom of Expression, Cybercrimes, Stakeholders, Perception, Impact

Introduction

Freedom of expression, while recognised as a fundamental universal human right, is guaranteed to varying extents across the globe depending on specific legal, political, and cultural contexts. Some countries, such as Norway and Denmark, rank highly for their strong protection of media freedom (RSF, 2024). In contrast, other African nations, such as Tanzania, face difficulties balancing this right with cybersecurity concerns. Tanzania's Cybercrimes Act No. 14 of 2015 has been criticised for restricting expression and impeding media freedom. Scholars such as Smith (2018) and Jones (2020) argue that although such legislation aims to prevent online offences, its vague definitions often lead to censorship and suppression of political dissent, particularly under authoritarian regimes.

Cybercrime laws worldwide tend to restrict freedom of expression due to vague definitions (Ajayi, 2016; Vese, 2022). Such legislation can either uphold or limit virtual rights (Gagliardone et al., 2018). Egypt and Indonesia have laws attempting to balance liberty and security (Fathy, 2018; Koto, 2021). EU experts mention conflicts with democratic values, such as surveillance issues, while Latin American specialists emphasise the need for legislative harmonisation with human rights. Asia differs; experts call for rights-based, detailed legislation to protect online freedom of expression. Chang (2020), Sombatpoonsiri and Mahapatra (2022), Batool (2022), and Aleem et al. (2021) highlight how restrictive policies, especially those during the pandemic, restrict free expression. Amro (2016) suggests balancing rights and cybersecurity, while Miller (2016) and Momen (2019) warn of censorship and insufficient protections. Aslan and Ercanli (2020) observe that, despite strict laws in Saudi Arabia and Qatar, privacy and free speech are compromised, raising human rights concerns.

The GCC nations have laws aimed at suppressing cybercrime, but these laws may also hinder political speech. Scholars such as Sairafi (2022), Gastorn (2017), Aissani (2022), and Ali (2021) call for reforms and regional cooperation to guarantee rights while maintaining cybersecurity. Nkongho (2016) observes that four of the top ten nations most impacted by cybercrimes are African countries. The African Union Convention on Cyber Security and Data Protection (AUCSCPDP) of 2014, which addresses issues such as how social media use influences freedom of expression (Ayalew, 2021), is in place. Hwang, Laing, & Holder (2016) explore state surveillance in Sub-Saharan Africa. Ashiru (2021) criticises Nigerian cyber stalking legislation, and Kakungulu & Rukundo (2019) acknowledge Uganda's involvement in digital activism. Snailka & Musoni (2023) evaluate South Africa's Cybercrimes Act. Laibuta (2022) and Ilori (2024) stress the importance of balancing cyberspace security with the protection of rights and freedom of expression across Africa.

The interaction between Cybercrime Acts and Freedom of expression from an East African perspective is enabled by the EAC Treaty and the East African Court of Justice (EACJ), both of which promote digital rights and good governance. Kirabira (2020) and Mugarura & Ssali (2021) note that the EACJ plays a fundamental role in balancing national law and human rights. However, Kenya, Uganda, Rwanda, Burundi, and Sudan's plural socio-political situations render it intricate to apply. Sugow, Zalo, & Rutenberg (2021) and Laibuta (2022) observe tensions amid freedom of speech and the enforcement of cybercrime law. Rwanda, Burundi, and Sudan's authoritarian digital policies illustrate the imperatives of cybersecurity law and the safeguarding of freedom of expression.

Researchers criticise Tanzania's Cybercrimes Act of 2015 for infringing on constitutional rights. Ndumbaro (2016) questions its compliance with Article 30, while Kirabira (2020) and Misso (2017) mention its adverse impact on journalists and privacy. Marere (2015) calls it detrimental to cyber speech, and Solomon (2022) holds it responsible for stifling citizen journalism in the COVID-19 era. Scholars call for immediate reforms to find a balance between cybersecurity and the protection of democratic freedom and human rights in Tanzania.

Statement of the problem

The article examines stakeholders' perceptions of the provision in the Cybercrimes Act No. 14 of 2015 of Tanzania that restricts freedom. Even though the Act was enacted to combat rising online criminal activities such as fraud, cyberbullying, and objectionable content, it has been a source of concern regarding its potential use to suppress fundamental freedoms. In the view of critics, the Act contains exceedingly wide and vague provisions, which permit subjective application and interpretation. These weaknesses have been consistently highlighted by legal practitioners, human rights groups, and media workers, and are replicated in comparable legislation in other regions of Africa. Mbunda (2020), for instance, notes that general terms such as "cyberbullying" and "spreading false information" have consistently been used to suppress political dissent and criticism.

In Tanzania, this is far from an academic issue: in 2016, Jamii Forums co-founders Mike William and Maxence Melo were arrested for refusing to reveal whistleblower identities, and in 2019, journalist Joseph Gandye was detained after reporting on alleged police brutality. While existing work, for instance, Ndumbaro (2016) and MCT (2022), is critical of the Act, it falls short of context-specific legal reform or empirical evaluation. Specifically, the role of police discretion in law enforcement is under-researched, which further increases freedom of expression. The law, if left unaddressed, can foster self-censorship among journalists, compromise democratic accountability, and harm public trust in online media. This study bridges these gaps through an empirical analysis of problem clauses, drawing on the perspectives of lawyers and journalists.

Objectives of the study

The objectives of the study are to find stakeholders' views on the sections of the Cybercrimes Act No. 14 of 2015 that infringe on freedom of expression in Tanzania.

Literature Review

Several studies have explored cyber laws in the East African region. Maghaireh's (2024) study on "*Cybercrime Laws in Jordan and Freedom of Expression: A Critical Examination of the Electronic Crimes Act 2023*" revealed that in Jordan, the increase of cybercrimes by the Act and, more ostensibly,

the "astronomical" punishments, with fines up to 75,000 JD when the average monthly salary is 543 JD, are most likely to instill extreme fear of draconian legal and financial sanction. Jordan's experience attests to the importance of legislative precision, proportionality, and compliance with international human rights standards to ensure that cybercrime legislation is not turned into an oppressive weapon but remains a rightful security tool.

Gyetvan (2024) and Popović (2021) noted that the lack of independent oversight bodies and the undermining of judicial independence embolden the misuse of cyber laws to suppress dissent. Ezeanokwasa (2019), Davis and Kleinhans (2017), and Zaichuk and Zaichuk (2019) note that foreign stakeholders view cybercrime legislation as a tool to shut down dissent and curb free speech. Abbas et al. (2023), Cross (2021), and Wright and Raab (2015) support global harmonisation to prevent state intrusion. Magalla (2017), Swetu (2022), and Okon and Udo (2019) report African grievances against comprehensive laws that restrict free speech. Sugow et al. (2021) and Njuguna (2018) discuss excessive vigilance in Kenya, but Mwangi and Ochieng (2020) echo the need to implement safeguards within East African legislation. Kagwe (2017) reports that legislation beyond stifles dissent and media freedom. Kamala (2019) and Mwanjala (2021) highlight negative determinants of freedom of expression in Tanzania that warrant legal reform.

Ademi (2024) provides a detailed analysis of Kenya and illustrates that, although Kenya has enacted several digital rights regimes, e.g., the Computer Misuse and Cybercrimes Act, most provisions of the latter, e.g., criminalising "false publications," are vaguely defined and utilised as weaponry against online activists, journalists, and ordinary citizens. Misso (2017) and Wajahat et al. (2025) call for greater judicial oversight and more inclusive legislative procedures to align the law with constitutional rights. Cross (2021) discusses Tanzania's growing draconian cyber legislation, illustrating how the State uses the Cybercrimes Act (2015) and associated regulations to blur the boundaries between digital criminality and dissent, and recognises a broader pattern of states practising digital authoritarianism, in which cybercrime law is employed as a political tool.

Helm and Nasu (2021), Ajayi (2016) noted that social media users who are critical of the State are consistently prosecuted under laws criminalising "seditious" content. Munezero (2024) comparatively examines freedom of expression laws across EAC member states and shows that while the legal jargon of most countries, including Rwanda and Uganda, acknowledges digital rights, practice often violates such commitments. Ndumbaro (2016), in "*The Cyber Law and Freedom of Expression: The Tanzanian Perspectives*", investigated how Tanzania's early cyber law regimes, particularly the Cybercrimes Act No. 14 of 2015, influence the constitutional Freedom of Expression. Ndumbaro discovered that a few provisions of the Cybercrimes Act, such as "*false information*," content regulation, and investigation powers, are ambiguous, overbroad, and open to abuse by state agents, likely to silence lawful speech.

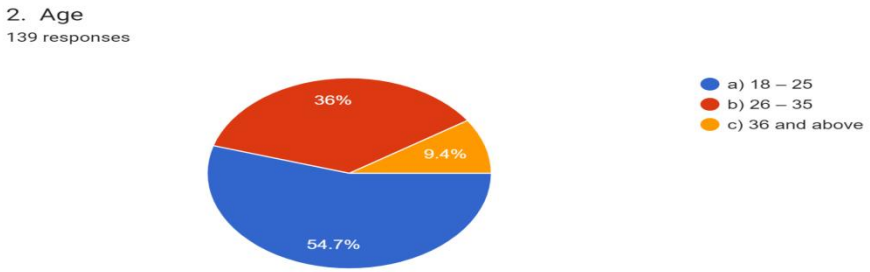
This paper fills a contextual gap by establishing the Act's impact in the aftermath of decades of enactment, giving a more balanced picture of its true effect on freedom of expression than Ndumbaro's earlier text-based method.

Methodology

To capture stakeholders' views on sections of the Cybercrimes Act No. 14 of 2015 that infringe upon freedom of expression, the study adopted a key informant interview method. The Mwanza Press Club (MPC) members constituted the study population, from which 22 members were selected. Twenty-two respondents, purposively selected, include legal experts and Journalism and Mass Communication lecturers. These respondents were chosen for their involvement in human rights activism, media law, and journalism. Interview responses were transcribed and were narratively and thematically analysed to elicit primary perspectives and overarching themes.

Data analysis and Presentation

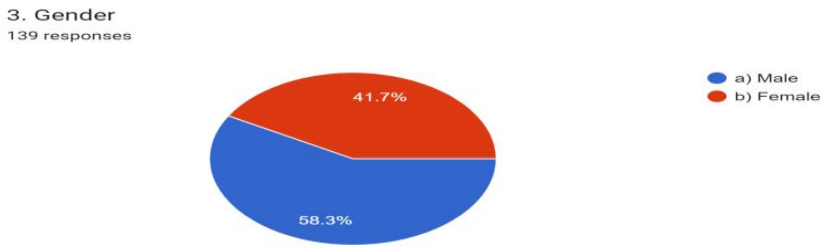
Figure 1: Age of Respondents



Source: Field Data 2024

The majority of respondents are young adults aged 18 to 25, indicating that the club's population is young and likely to influence the club's perspectives and activities. The absence of members aged 36 and above suggests a potential lack of experience and/or diversity of opinion.

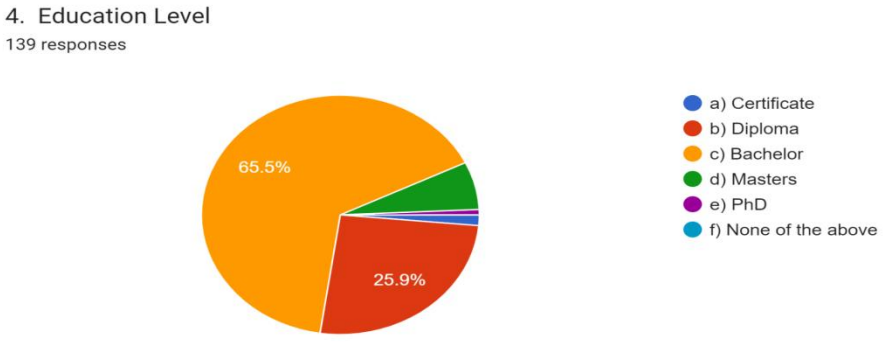
Figure 2: Gender of respondents



Source: Field Data 2024

Male members constitute 58.3% of the total, which demonstrates a gender gap. Such gender imbalance may limit the boundaries of discussions and, therefore, the absence of the female voice may be more pronounced.

Figure 3: Respondents' Education Level



Source: Field Data 2024

The respondents are highly educated, as evidenced by the 65.5% holding a bachelor's degree. This indicates that the club has significant pedagogical capital and can dissect the topic under study.

Discussion

The Arrest and Disappearance of Journalists and Citizens

Interviews with respondents indicated that the law has resulted in arrests and disappearances. Respondents believe. Since its enactment in 2015, the Cybercrimes Act has been used repeatedly to arrest journalists, opposition leaders, and ordinary citizens. These acts have generated severe chilling effects on freedom of expression in Tanzania. For example, one of the respondents said:

> I am sure you remember one of the most prominent cases prosecuted under this Act: that of Maxence Melo, the co-founder of Jamii Forums, who was arrested and charged several times between 2016 and 2018. Authorities accused him of violating Sections 16 (false information) and 32 (disclosure of data) after he refused to hand over users' private information and allegedly published false content. You are a journalist too, and you know that the ethics and etiquette of our profession do not allow us to expose anonymous sources. That is exactly what Mr Melo defended, and although he eventually won the case with the support of human rights activists, can we really believe that every journalist in Tanzania has such connections? What if law enforcers succeed in prosecuting you before activists can intervene? You see, Melo's repeated harassment clearly illustrates how this law can be used against digital platforms that promote accountability (MPC5, December 3rd, 2024).

One of the Legal Experts E1 noted:

> The application of the Cybercrimes Act in several cases demonstrates its potential to restrict freedom of expression in Tanzania. While combating cybercrime is important, the misuse of this law to suppress critical voices undermines democratic principles and human rights. (E1 December 9th, 2024).

One lecturer also said:

> Since the enactment of the Cybercrimes Act, many media outlets, journalists, and communication professionals have faced significant challenges. For instance, Maxcence Mello, Mwananchi Digital, Clouds Media, Wasafi, and Mwanahalisi are just a few of the numerous media entities affected by the Act. As an academician, I find the Cybercrimes Act deeply troubling for journalism and media studies. We are raising graduates who choose silence over truth, not because of a lack of ideas, but because the law criminalises their voice" (L3, December 3rd, 2024).

MPC41 also added:

> I attended an event in Mwanza on Press Freedom Day. One of the key speakers cautioned journalists, saying, 'There is no sweeter story than your Life as a journalist.' What does this mean? The disappearance and harassment of journalists under this Act make us feel invisible and powerless. I recall the arrest of a young student in 2017 for a satirical Facebook post; this shows that the law is not only targeting seasoned reporters but also ordinary citizens. (MPC41, December 2024).

Respondents attested to several instances of how the Cybercrimes Act No. 14 of 2015 has been used to curb freedom of expression in Tanzania, and most often against individuals exercising their constitutional rights of free speech. Misuse of vague provisions in the law, particularly Sections 14 and 16, shows how the Act is used to address real cyber threats, suppress dissent, silence critics, and control public discourse. Researchers such as Wiener (1958) and Schauer (1978) have warned of horrific outcomes in which actors or institutions shy away from open discussion in fear of the State acting against them. Another example was that of a Mwanahalisi reporter, who had written on a purported misdeed by government officials. It resulted in charges against him under Section 16 for false publication. He was arrested, interrogated, and held for days without trial, with the reverberations of the argument by Abbas et al. (2023) that vaguely worded legislation is usually used to muzzle media critical of the State. This revelation is contrary to those of Maghaireh (2024) and Ezeanokwasa (2019), who

establish that expansive definitions of cybercrime acts are often used to silence minority opinions in the guise of morality or national security.

Limited Understanding of the Law among Citizens and Journalists

Interviews conducted under this objective revealed limited understanding and awareness of the Cybercrimes Act No. 14 of 2015 among stakeholders. A respondent from the group of Legal Experts said:

> The Cybercrimes Act No. 14 of 2015 is the only Act in Tanzania to have been passed at midnight by very few members of parliament and even fewer ministers. The parliament participants were very tired. The day began with the discussion and passage of many bills, and finally, the Cybercrimes Act was discussed; it was passed at midnight. Not a single member from the ruling party disagreed with any section of the Act. I only saw Munyika, Lissu, and Mdee fighting to stop the bill, especially to address vague terminologies and heavy, unrealistic penalties, but they ended up being booed by members of the ruling party. It was very cold in the building, and I saw Lissu chewing a menthol candy to stay warm (E1, December 7th, 2024).

Another respondent from the group of lecturers noted:

> As an academician, I find one of the biggest threats posed by the Cybercrimes Act is not only its vague provisions but also the limited understanding citizens and journalists have of what it actually contains. Many of my students assume every online post can lead to prosecution, and that fear bleeds silence. **(**L1, December 9th, 2024).

Legal expert E4 said:

> In my court experience, many accused persons admit they never knew their WhatsApp messages or tweets could be treated as criminal offences. Journalists especially misunderstand the thin line between investigative reporting and 'false information' **(E4, December 12th, 2024).**

However, findings from questionnaires completed by Mwanza Press Club (MPC) members indicated that the majority of respondents (52.9%) are familiar with the Cybercrimes Act. This suggests that over half of the participants have a good understanding of the Act and its implications. A significant proportion (26.8%) admitted knowing something about the Act. A smaller percentage (10.9%) admitted not knowing the Cybercrimes Act. The lowest rate (9.4%) agreed that they were very much aware of the Cybercrimes Act. These figures on the findings indicate a fairly high level of acquaintance among interviewees, and 79.7% (Familiar + Somewhat Familiar) suggest at least some knowledge of the Act. This shows that the majority of the respondents made useful contributions to the research. Being 10.9% Not Familiar reminds one that awareness and capacity-building should be undertaken so that everyone understands the law's impacts.

According to the Chilling Effect Theory, fear of legal sanctions or doubt may deter an individual from exercising their right to free expression. Ndumbaro (2016) observes that although the Act purports to enhance cyber security, it is likely to be beleaguered with problems when enacted to stifle resistance and public discourse, and hence walk all over constitutionally protected liberties. The participants validate existing research, such as Cross (2021) and Magalla (2017), which is negative about the Act's elastic and loose provisions in constructing a framework for a legal regime in which self-censorship is normalised and to which journalists habituate themselves. The 10.9% of respondents who answered that they did not know about the Act indicate an increased failure of legal literacy among media practitioners. As noted by Swetu (2022), the lacuna exposes journalists to undue abuse and incapacitates them from effectively resisting the abuse of law. This is also the reason why digital rights training and legal education are necessary, as posited by Misso (2017). These findings are in line with Wiener's (1958) Chilling Effect Theory, which asserts that anomalous or punitively stringent laws discourage

individuals from exercising their right to free expression, even when what they are expressing is legal. The midnight parliamentary approval of the Act, with little opposition and inadequate scrutiny, validates the concerns expressed by Zaichuk and Zaichuk (2019), which indicate that rapidly shifting digital law is prone to precede democratic debate and produce open-ended provisions that facilitate state misuse. Collectively, these findings show that limited stakeholder engagement, driven by unclear legal jargon, creates a culture of fear, silence, and reduced civic participation, underscoring the compelling need for reform aligned with international human rights standards.

False Information

The interview with respondents reveals that Section 16 of the Cybercrimes Act No. 14 of 2015, which criminalises the spreading of false information, poses serious consequences on Tanzanian press freedom. Stakeholders understand that, while the section ostensibly aims to prevent disinformation and protect the public from dangerous falsehoods, its broad, vague language has actually hindered journalists' freedom to report and practice investigative journalism. For example, legal professionals categorise the respondent mentioned:

> For journalists, the ambiguity of this provision makes it unclear which types of information would be barred, leading to blanket self-censorship. That is why journalists tread on eggshells when reporting controversial or sensitive news, because they do not want their reporting to be alleged to be propagating "false information" and to be severely punished. The draconian punishments listed under Section 16, i.e., imprisonment and substantial fine, encourage this chilling effect. The docility undermines the media's watchdog function against corruption, its role as an official watchdog, and its role as a people's educator in matters of public interest (E12, November 12th, 2024).

But one of the lecturers, L5, had this to say:

> I want to say that while combating the spread of false information is a legitimate issue, Section 16's current use has a disproportionate effect on journalistic freedom. Reforms must find a balance between accountability and protecting free expression. Objective and clear premises on which false information would be regarded should be established, based on proven-to-be-false materials, malevolently created, and causing serious damage. (L5, December 18th, 2024).

Contributors spoke of how a lack of precision in the defining words has led to rampant self-censorship among media professionals, citizen reporters, and social media users. This is borrowed from Wiener's (1958) Chilling Effect framework, in which unclear legislation deters legitimate expression in fear of punishment. Likewise, Zaichuk and Zaichuk (2019) note that weakly written cybercrime laws worldwide are used by governments to silence dissent, and the Tanzanian experience follows, where critical media reporting has the potential to be branded illegal. The accounts also align with Sugow et al. (2021), which document similar curtailments in Kenya under cyber-harassment legislation, illustrating how governments use legal loopholes to harass media professionals. While participants emphasise the law's abusive application, L5's call for reforms that distinguish malicious disinformation from good-faith journalism offers a positive avenue forward. This is in line with international best practice but less urgent in comparative literature, which is more likely to focus on repression rather than examine reform strategies. In addition, Abbas et al. (2023) mention enforcement capacity structural vulnerability, whereas Tanzanian stakeholders suggested selective over-enforcement, swiftly applied against critics yet ineffective against genuine cyber threats.

Offensive Communication

The respondents' interviews concluded that Section 14 of the Cybercrimes Act No. 14 of 2015, which criminalises offensive online communication, has had a significant impact on Tanzanian journalists when writing opinions and reporting sensitive matters. Stakeholders asserted that, even though the section was enacted to prevent harmful and insulting online behaviour, its vagueness and susceptibility

to abuse have curtailed journalistic freedom and silenced public discourse. A stakeholder among the team of legal experts claimed:

> My biggest problem with Section 14 is that the definition of offensive communication is open and vague. For journalists, this legal uncertainty fosters a climate of fear and self-censorship, discouraging them from broaching sensitive topics or broadcasting opposing views. (E1, December 7th, 2024).

Another legal commentator, E2, also contained:

> Reporters avoid writing about politically sensitive topics, corruption, or social issues for fear of taking legal action. Legal action has been pursued against reporters and media outlets that have been put on trial for articles deemed critical of government officials or other influential figures. The climate dissuades good journalism, undermining the media's ability to foster transparency and accountability (E2, December 10th, 2024).

Amongst one of the members of the Tanzania Editors Forum, F1 was of the following views:

> This story, although intended to counter online abusive and dangerous behaviour, this part's vague and extremely general language has created tremendous room for random use. Research participants noted that the ambiguity around what constitutes offending content has led journalists to engage in wide-ranging self-censorship (F1, December 14th, 2024).

An analysis of Section 14 of the Tanzania Cybercrimes Act No. 14 of 2015 demonstrates how criminalised offensive communication legislation has limited space for public discourse and media freedom. This is complemented by Wiener's (1958) Chilling Effect theory, which holds that loose legal perimeters deter people from exercising their rights to avoid prosecution. In reality, Tanzanian journalists avoid writing about corruption, government collapse, or dangerous topics if their reports are deemed "*offensive*." These findings validate Zaichuk and Zaichuk's (2019) argument that vague cybercrime legislation facilitates selective enforcement, most commonly against oppositional voices within power's grasp. These trends have also been reported by Maghaireh (2024) in Jordan and by Wajahat et al. (2025) in Pakistan, where legislation on offensive or hurtful communications has been used to censor investigative reporting and silence critics.

Self-Censorship

Surveys of stakeholders indicated that the Cybercrimes Act No. 14 of 2015 has played a significant role in encouraging self-censorship by both journalists and citizens in Tanzania. According to respondents, the possibility of prosecution under the Act's vague and restrictive provisions has had a chilling effect, leading citizens and journalists to refrain from publishing or reporting sensitive or controversial topics. The findings were that self-censorship deters the media from performing its constitutional function of facilitating transparency, accountability, and public debate. The following is from a respondent among a group of lecturers:

> Among the key reasons for self-censorship is the ambiguity of the Act's provisions, including those on offensive communication and the dissemination of false information. Such legal ambiguity, coupled with the draconian consequences of non-adherence, such as imprisonment and large fines, has prompted journalists to take the easy way out, at times at the cost of tough journalism (L6, November 20th, 2024).

Meanwhile, among the legal experts E6 included:

> The Cybercrimes Act has created an environment in which journalists and whistleblowers increasingly practise self-censorship. By silencing loud critics and constraining media freedom of reporting, the Act works against the principles of an independent and free press. (E6, November 14th, 2024).

TEF F2 said this:

> Do you ever wonder why journalists and lawyers today prefer to use WhatsApp calls and messages? It is because of the Cybercrimes Act No. 14 of 2015, if I may say so. Individuals who are aware of the Act avoid using common text messages or phone calls to communicate issues they think could be tapped and used against them under this Act. Its victims are unaware of its implications, particularly how their lives can be affected once they have posted content that qualifies as false or untrue (F2, December 14th, 2024).

Findings from a questionnaire administered to Mwanza Press Club members revealed that self-censorship is common, with 139 respondents providing their views. Over half (50.4%) admitted to self-censorship. A smaller but significant proportion (33.1%) reported zero experience of self-censorship. 16.5% were unsure. The results suggest that self-censorship has become a considerable obstacle to press freedom, notably in sensitive or contentious reporting. The results confirm Wiener's (1958) and Schauer's (1978) Chilling Effect theory, which holds that vague and repressive laws induce fear, suffocating legal speech. The same trends are also found outside the country: Helm and Nasu (2021) find that imprecise speech laws allow risk-averse reporting, while Khan et al. (2019) have found similar effects in Pakistan under PECA-2016.

The report supports the view that undue punishment and substandard provisions have instilled fear among people and journalists and restricted free expression. L6's description of a journalist shelving a scoop after one of their colleagues was taken to court is a living testament to the toll this takes on people at work. Comparative studies confirm these accounts. Abbas et al. (2023) and Khan et al. (2019) report the same practice under PECA-2016 in Pakistan, where loose cybercrime laws gagged journalists. Burton (2019) supplements this by reporting oppressive cyber law as a means of "virtual occupation," a trend copied in Tanzania, where the Cybercrimes Act is reported to police online space through intimidation. Helm and Nasu (2021) also warn that poorly designed countermeasures to "fake news" were found to violate international human rights standards, in line with respondents' calls for a definition and a proportionate penalty.

Teaching and Curriculum Impact

The stakeholder interview acknowledged the Cybercrimes Act's power to foster internet discipline and digital safety. In general, this research appreciates the important role the Act plays in Tanzania in safeguarding digital infrastructure, protecting sensitive information, and combating cybercrime. Respondents revealed that the existence of the Cybercrimes Act has disciplined people who previously had a habit of speaking recklessly and sharing everything on social networks without considering the truth or accuracy of the information they were spreading online. According to the findings, the rise of social media turned Tanzanians into naive individuals, mindlessly following trends and putting everything online as if the whole country were a place of entertainers seeking followers. At some point, even a minor dispute with a neighbour or relative would expose an individual’s weaknesses on social media, along with false accusations, to portray the victim as an unworthy member of society. One of the respondents from the group of lecturers L5 expressed how good the Cybercrimes Act is, saying:

> I personally thank the government for enacting this Act, as it has instilled discipline in people. A bit of recklessness now leads to prison time and fines. The law has helped curb irresponsible use of social media among Tanzanians (L5, November 20th, 2024)

Another lecturer L2 said:

> Our Journalism and Mass Communication universities and colleges are currently producing ‘chawa’ journalists. These are journalists who have earned degrees, diplomas, and certificates with good grades but fail to practise professional journalism because of draconian laws that infringe on freedom of expression in our country, such as the Cybercrimes Act. They are graduates seeking employment, but employment is often given to journalists who beautify the authorities. Our graduates in Journalism and Mass Communication currently practise sycophantic journalism. Purely praising those in power and tycoons, unnecessarily. As their lecturers, we have encountered them in several workshops, and when we question what they are doing, they often respond by citing restrictive media laws. Cybercrimes included, and poverty. (L2, November 3rd, 2024).

However, members of the Mwanza Press Club (MPC) informed the media organisations through a questionnaire that they have amended their policies in line with the Cybercrimes Act. The 138 responses show the rates of policy change experienced by the respondents. Most respondents (73.9%) reported experiencing changes in their organisation's editorial policies since the Act came into effect. A small but noticeable proportion (17.4%) indicated radical changes in editorial policies. Very few respondents (8.7%) reported no policy change in their organisation's editorial policies. The findings suggest that the implementation of the Cybercrimes Act has elicited widespread reformulation of editorial policies, and 91.3% of respondents (comparing "Some Changes" and "Significant Changes") have reported changes.

This suggests that the Act has had far-reaching effects on how media companies conduct their business, including how they report on content creation and sharing. These profound changes highlight the Act's far-reaching impact, particularly in settings where aversion to risk is desirable, leading to what Schauer (1978) and Wiener (1958) called a chilling effect, whereby the threat of legal penalty causes self-censorship and limits the scope of safe expression. This aligns with Helm & Nasu (2021)'s evaluation of how "fake news" legislation can reshape media behaviour. Cumulatively, an overwhelming 91.3% of respondents ("some changes" and "significant changes") acknowledge direct policy changes resulting from the Cybercrimes Act.

International Standards Agreement

Results from an interview with respondents indicated that the Tanzanian Cybercrimes Act No. 14 of 2015 has a significant divergence from international standards on freedom of expression. Although the Act seeks to address genuine issues in cybersecurity and cybercrime, its broad and prohibitive provisions are largely inconsistent with the standards established in international human rights instruments. For example, a legal expert E7 said:

> It is totally wrong to compare this Cybercrimes Act with international human rights standards, because it does not comply with international treaty obligations, such as the International Covenant on Civil and Political Rights (ICCPR) and the African Charter on Human and Peoples' Rights (ACHPR). If you go through these documents, you will see that, for example, the International Freedom of Expression standards highlight that any restriction must meet the tests of legality, necessity, and proportionality. This cannot be found in our Cybercrimes Act. (E7, November 15th, 2024).

Lecturer L1 added:

> International norms favour the protection of those who disclose corruption, human rights abuse, or other matters of public interest. Not incorporating such protection into the Cybercrimes Act exposes individuals to prosecution for acts essential to democratic accountability and active public discussion (L1, December 5th, 2024).

According to the findings, International Human Rights law stipulates that any restriction on expression must be lawful, necessary, and proportionate. Maghaireh (2024) and Runa (2019) add that such punishments deter vital democratic practices, such as investigative journalism and dissident speech, which run counter to the principle of proportionality under international law. Interviewees emphasised the absence of judicial oversight, particularly regarding surveillance and data access, and expressed serious concern about unfettered state power. As Abbas et al. (2023) and Ajayi (2016) argue, this undermines public trust and accountability, especially where the judiciary does not independently review civil-liberty-curtailing measures. In addition, the Act does not have express protection for whistleblowers and journalists, who are persecuted for revealing corruption or mismanagement. This failure, also cited by Zaichuk & Zaichuk (2019) and Ndumbaro (2016), violates international best practice in safeguarding persons working to ensure openness and good governance.

Stakeholder Engagement

The interview with stakeholders revealed that, to some extent, the process of establishing the Cybercrimes Act engaged experts and stakeholders. The main concern raised by respondents was that, even among those involved, some of their critical views, opinions, and contributions were neither considered nor included in the Act. For example, a lecturer L2 said:

> The problem in our country is that when you talk about journalists, you often mean those residing in Dar es Salaam. When it comes to issues that require journalists as stakeholders to share their views, the government almost always considers only those based in this major city. I do not mean to suggest that these journalists are uninformed, but ignoring the perspectives of journalists from other cities or regions is unprofessional. Including such overlooked journalists could help address what is happening now, where stakeholders of the Cybercrimes Act are expressing complaints. Even those in Dar es Salaam have stated that their suggestions were not considered, which is why they, too, are criticising the Act for infringing on their right to freedom of expression (L2, November 3rd, 2024).

Moreover, lecturer L1 noted:

> In my view, the poor engagement of stakeholders, such as journalists, during the drafting process has even led to a lack of familiarity and appreciation of the Act among journalists. This has created a confrontational environment, with the media perceiving the law as something to be endured rather than as a tool to encourage responsible reporting and Internet security (L1, December 9th, 2024).

Another L4 lecturer added:

> The limited media and stakeholder coverage during the drafting and enactment of the Cybercrimes Act has led to a negative perception of the law and its capacity to function without obstruction. (L4, December 1st, 2024).

These findings resonate with Scholars such as Runa (2019) and Sugow et al. (2021), who argue that ambiguous cybercrime laws drafted in the absence of stakeholders are systematically used as weapons of attack against the media and civil society. Wajahat et al. (2025) observed that upper-level legal structures, especially those with unclear provisions, tend to facilitate online censorship and suppress public-interest journalism. This exemption has also had far-reaching implications, as observed by Lecturer L2, who noted that the journalists were not involved and given a chance to participate in the legislative structure. Ndumbaro (2016) finds that media players' exclusion from policymaking strengthens law enforcement. Without direction or involvement, the majority of Tanzanian journalists are unaware of the scope and legal complexities of the Act, interpreting its operation out of fear rather than logical understanding, thereby imposing a chilling effect under Wiener (1958) and Schauer (1978). Engaging media professionals, lawyers, civil society, and digital rights activists would not only enhance trust and accountability but also result in a balance, democratic model catering to both cyber security and freedom of expression requirements according to the International Covenant on Civil and Political Rights (ICCPR) and the African Charter on Human and Peoples' Rights (ACHPR) (Zaichuk & Zaichuk, 2019; Maghaireh, 2024).

Vague and Overly Broad Provisions

During interviews with stakeholders, it was revealed that the Cybercrimes Act No. 14 of 2015 contains provisions that are overly broad and vague, thereby prone to abuse and misuse. Respondents held the view that the provisions have far-reaching effects on freedom of expression in Tanzania, as they lead to self-censorship and vagueness and can be used discriminatorily to suppress dissenting voices, activists, and journalists. For example, one legal expert E5 said:

> On my side, I can say that the worst of such objectionable provisions is Section 16, which criminalises the dissemination of false information. False information is not defined in

> the Act and is left to personal interpretation. This breadth discourages individuals from speaking out on controversial issues out of fear of prosecution. (E5 December 13th, 2024).

Another interviewee, a member of the Tanzania Editors Forum (TEF), F2, said:

> My view is that several terms in the Act are not well defined; these terms create subjective conditions rather than objectivity. For instance, Section 18, relating to xenophobic and racist material, is another area open to misuse. Although combating hate speech is necessary, no regulations under this section endanger targeting legitimate debate (F2, December 14th, 2024).

However, lecturer L8 had this to say about undefined terms of the Act:

> In my view, these undefined terms in the Cybercrimes Act result in self-censorship, whereby organisations and individuals are hesitant to publish or share information that could be deemed misleading, offensive, or damaging (L1, December 9th, 2024).

According to findings from stakeholder interviews, vagueness in the Act gives officials too much power to prosecute as criminal dissent, satire, or investigative reporting, even when based on facts. This situation creates chilling effects on the beneficiaries of the Act, thereby hindering freedom of expression. Abbas et al. (2023), Gyetvan (2024), and Wajahat et al. (2025) agree that such room for manoeuvring in law leaves scope for political repression and the gagging of critical speech. Moreover, Sections 31 and 32 authorise police to take away information on flimsy grounds of "reasonable suspicion," which undermines privacy rights and enhances the sense of being watched, replicating the concerns of Popović (2021) and Zaichuk (2019).

Disconnection between the Law's Purpose and Reality

The stakeholder interview revealed that the purpose of the Cybercrimes Act No. 14 of 2015 appeared to be controlling detrimental behaviour in cyberspace, protecting citizens against cybercrime, and maintaining public order within the cyber community. For example, some of the stakeholders said that the Act does not favour Tanzanians but rather foreigners, noting that foreigners' stolen phones are detected so easily and in a short period of time, unlike Tanzanians, where the majority are completely not found, and a citizen is supposed to pay the police officer to investigate their stolen phone. A legal expert E4 said:

> I have witnessed this first-hand. Recently, a foreigner's phone was recovered within 30 minutes of being stolen, while others have waited years without success. Yet, if a foreigner or someone influential is affected, the police's Cybercrimes Unit acts with incredible efficiency. This Act must undergo major reforms. It has largely failed, as seen with the growing prevalence of scams like "pay via this number." If the Act cannot apprehend these perpetrators, what is its purpose? How can we protect our children from child pornography when we allow the promotion of homosexuality online? The Cybercrimes Act does not include provisions to prevent such content. Without seminars educating social media users, both young and old, on responsible use and meaningful protection, meaningful protection is impossible (E4, December 12th, 2014).

However, lecturer L4 said:

> In my view, the intention does not match the reality. If the course is to serve a purpose, the Act must be overhauled on revolution lines. First, open-ended language in such provisions as this should be tightly defined so that it targets dangerous activity without trespassing on constitutional protections (L4, December 1st, 2024).

According to the findings, there is significant misalignment between legislative intent and its practical

impact on freedom of expression. Although the Act seeks to combat disinformation, cyberbullying, and hate speech, its vague and extremely wide-ranging provisions have been systematically exploited in fact to harass, intimidate, and silence journalists, activists, and regular citizens who criticise government misconduct or dissent. Such a usage is in line with the warnings of Wiener (1958) and Schauer (1978), who advise that broadly worded statutes are likely to have a "chilling effect," which inspires fear, silence, and withdrawal from public debate. As Legal Expert E4 states, even though the intent behind the Act is laudable, its real-world impact tends to run counter to the spirit of freedom of expression. As Ajayi (2016) rightly points out, inadequacies in legal consciousness tend to lead to the abuse of cybercrime legislation.

Conclusion

This paper explored stakeholders' views on how Tanzania's Cybercrimes Act No. 14 of 2015 restricts freedom of expression. Findings show that the Act infringes freedom of expression, as noted by Journalists, legal experts, and academicians teaching Journalism and mass communication. They collectively agreed that while the Act addresses cyber threats, some of its provisions pose serious risks to democratic rights—vague terms lead to arbitrary enforcement and self-censorship, thereby undermining press freedom. The primary concern was a lack of judicial oversight, particularly regarding surveillance and data access, which compromised privacy protections and public trust. Stakeholders called for legislative specificity, proportionate punishment, and reparative justice to prevent excessive punishment of trivial offences. Stakeholders also called for legislative protections specific to journalists and whistleblowers, who are prosecuted for advocating transparency. In practice, this study emphasises amending the Act to ensure judicial accountability, legal accuracy, and conformity with constitutional rights and international human rights standards.

Recommendations

The study confirmed that Tanzania's Cybercrimes Act No. 14 of 2015 contains provisions incompatible with international human rights principles and constitutional protection. Most notable among them are the lack of judicial review, pursuant to which enforced disappearances, arbitrary detention, and abusive monitoring have been carried out. The study demands reforms to ensure the Act aligns with international standards of legality, necessity, and proportionality, particularly in regulating online media. Surveillance, access to information, and arrests under the Act must be subject to judicial oversight to ensure checks and balances and human rights protection.

The research also established that disproportionate punishment under the Act has led to widespread self-censorship and intimidation. It thus calls for the protection of journalists, whistleblowers, and members of civil society by law, and for proportionate and reasonable punishment for acts of wrongdoing. Also, the process of drafting the Act involved little consultation with interested parties. Therefore, future reforms need to adopt open and inclusive processes that affect the public, civil society, lawyers, and the media. The second most striking observation was low legal literacy among citizens and journalists, which renders them susceptible to the abuse of their rights. The study champions government-sponsored legal studies courses held jointly with NGOs and schools. Finally, ambiguous language and harsh penalties under the Act deter freedom of expression online. The study recommends that the Act be amended to include specific definitions and adopt a Customised Model that reflects the nature and seriousness of actual cybercrimes. These reforms are intended to ensure that the Cybercrimes Act protects the public interest while advancing human rights and democratic freedoms.

References

Abbas, Z., Khan, R., Khan, M. Z., & Imran, M. (2023). Cyber laws and media censorship in Pakistan: an investigation of governmental tactics to curtail freedom of expression and right to privacy. *Journal of Creative Communications*, 09732586231206913.

Abdulrasaq, K. (2025). Cyber Security and Right to Free of Speech; Analysing the Implication of Cyber Security Measures on Freedom of Expression and Access to Information. *Analysing the Implication of Cyber Security Measures on Freedom of Expression and Access to Information*.

Acosta, L. (2020). Efforts to align Latin American cybercrime laws with global free speech Standards: Analysing broad regulations on computer crimes and their implications for freedom of expression. *Journal of Cybersecurity and Privacy*, 12(3), 123-145.

Adibe, R., Ike, C. C., & Udeogu, C. U. (2017). Press Freedom and Nigeria's cybercrime act of 2015: An assessment. *Africa Spectrum*, *52*(2), 117-127. *African Legal Studies*, 7(2), 78-94.

Aissani, N. (2022). The influence of international law on Middle Eastern cybercrime policies. Journal of Global Cyber Law, 8(2), 133-152.

Ajayi, E. F. G. (2016). Challenges to enforcement of cyber-crimes laws and policy. *Journal of Internet and Information Systems*, *6* (1), 1-12.

Aleem, A., Asif, M., & Ashraf, R. (2021). Criticism of Pakistan's Prevention of Electronic Crimes Act: Ambiguity and broad scope limiting online freedom. *Journal of Asian Cyber Legislation*, 8(3), 145-167.

Ali, S. (2021). Comparison of cybercrime legislation enforcement in GCC and ASEAN: Evidencing complex dynamics between cybercrime laws and freedom of expression. Asian-Middle Eastern Journal of Cyber Law, 9(3), 178-195.

Amro, A. (2016). The need for cybercrime legislation that secures e-government and private Sectors while safeguarding expression. Middle Eastern Journal of Cyber Law, 4(2), 45- 67.

Aslan, H., & Ercanli, T. (2020). Strict online regulations in Saudi Arabia and Qatar and their limitations on expression. *Arabian Journal of Cyber Regulations*, 11(2), 159-176.

Awad, A., & Mburu, D. (2017). African legislative reforms with clear definitions to prevent Misuse: Stressing regional cooperation. *African Journal of Legal Reform*, 11(3), 112-128.

Ayalew, B. (2021). The impact of the African Union Convention on Cyber Security and Data Protection (AUCSCPDP) on online freedom of expression. *African Journal of Cyber Law*, 9(1), 72-89.

Ashiru, A. (2021). Cyberstalking law and the right to freedom of expression in Nigeria: A dead Ringer or a constitutional snag? *Available at SSRN 5197981*.

Balkin, J. M. (2015). The dual role of cybercrime laws: Balancing threats and avoiding overreach that stifles free speech. *Journal of Cyber Law and Policy*, 7(2), 55-73.

Batool, Z. (2022). Ethical challenges in balancing free expression and controlling online hate Speech in South Asia: Analysis of strict penalties against hate propaganda. *South Asian Journal of Ethics in Cybersecurity*, 6(1), 78-95.

Bradshaw, S., Bailey, H., & Howard, P. N. (2021). Country case studies industrialised Disinformation: 2020 global inventory of organised social media manipulation. *Journal of Information Policy and Regulation*, 17(2), 134-150.

Chang, Y. (2020). Examination of Northeast Asia's cybercrime laws: A comparison with Europe's Budapest Convention on cybercrime and its implications on expression and privacy. *Asian Journal of Cyber Law*, 15(2), 112-134.

Christou, G. (2018). The challenges of cybercrime governance in the European Union. *European Politics and Society*, *19*(3), 355-375. Creswell, J. W. (2021). Sampling techniques: *Journal of Sampling and Research Methods*, 15(3), 78-94.

Chuma, W. (2018). Restricting media freedom in Southern Africa through cybercrime legislation. *Southern African Journal of Media and Law*, 9(2), 77-93.

Ekwe-Ekwe, H. (2019). Cybercrime legislation in Africa: Protecting users while avoiding political repression. *African Journal of Cybersecurity and Law*, 11(3), 123-140.

Ezeanokwasa, J. O. (2019). Child Pornography under the Cybercrimes Act 2015 of Nigeria: The Law and Its Challenges. *AFJCLJ*, *4*, 94.

Fathy, N. (2018). Freedom of expression in the digital age: enhanced or undermined? The case of Egypt. *Journal of Cyber Policy*, *3*(1), 96-115.

Gagliardone, I., Gal, D., Alves, T., & Martinez, G. (2018). Cybersecurity and media Freedom in Africa. Journal of African Media Studies, 10(1), 23-45.

Gastorn, L. (2017). Regional and international law impacts on Middle Eastern cybercrime legislation. *International Journal of Law and Cyber Policy*, 6(1), 53-75.

Gyetvan, D. (2024). Censorship and Freedom of Expression in the Age of Social Media. *ELTE LJ*, 27.

Helm, R. K., & Nasu, H. (2021). Regulatory responses to 'fake news' and Freedom of Expression:

normative and empirical evaluation. *Human Rights Law Review*, *21*(2), 302-328.
Ilori, T. (2024). A postcolonial legal critique of online expression in Africa. *Journal of African Law, 68*(3), 283–300.
Kagwanja, P. (2017). The negative impact of cybercrime laws on digital activism: Urging reforms. *Journal of Digital Activism and Law*, 8(1), 123-139.
Kakungulu-Mayambala, R., & Rukundo, S. (2019). Digital activism and free expression in Uganda. *African Human Rights Law Journal, 19*(1), 167–192.
Kashonda, C. (2018). The dual role of Tanzania's Cybercrimes Act: Balancing security and free speech. *Tanzanian Journal of Digital Law, 12*(1), 145–162.
Kimaro, S. (2019). The need for amendments and regular reviews of Tanzania's Cybercrimes Act to Balance security and free speech. *Journal of Digital Policy and Regulation in Tanzania*, 14(3), 198-215.
Kirabira, T. R. (2020). New digital media: Freedom of expression and safeguarding journalists in the Context of East Africa. *Cross-cultural Human Rights Review, 2*(1), 39–57.
Khan, S., Tehrani, P. M., & Iftikhar, M. (2019). Impact of PECA-2016 provisions on freedom of speech: A case of Pakistan. *Journal of Management Info, 6*(2), 7–11.
Koto, I. (2021). Cyber crime according to the ITE law. *International Journal of Reglement & Society, 2*(1), 32–40.
Laibuta, M. (2022). Constitutions, freedom of expression, internet shutdowns, social media and defamation laws in Africa. In *Comparative constitutional law in Africa* (pp. 268-291). Edward Elgar Publishing.
Lema, G. G. (2024). Free space optics communication system design using iterative optimisation. *Journal of Optical Communications, 44*(S1), S1205–S1216.
MacKinnon, R. (2017). Safeguarding digital infrastructure and user rights: The necessity of clear legal frameworks that respect human rights. *Journal of Digital Rights and Law*, 9(1), 88-104.
Maghaireh, A. M. (2024). The Legal Nature of Cyberbullying: A Comparative Study Between the American and the Jordanian Laws. *UAEU Law Journal*, *2024*(98), 4.
Maillart, P. (2019). Cross-jurisdictional challenges in prosecuting cybercrimes. Journal of Cybersecurity, 5(3), 233-250.
Magalla, A. (2017). Human Rights Protection in Tanzania as Described by the Cyber Crime Act, No. 13 of 2015.
Marere, J. (2015). The Cybercrimes Act, 2015: A Weed in the Garden of Freedom of Expression in Tanzania. *Masters dissertation, Mzumbe University*.
Mawere, M., & Mutasa, M. (2020). Balanced laws to protect against cyber-attacks while upholding free speech. *Journal of Cybersecurity in Africa*, 13(4), 112-129.
Mbatha, M. (2019). *Vague cybercrime laws in Africa: Suppressing free speech and targeting activists.* African Journal of Legal Studies, 11(1), 132–148.
Mbilinyi, S. (2017). Specific reforms to Tanzania's Cybercrime Act, including periodic reviews. *Tanzanian Journal of Legal Reform*, 10(3), 99-115.
Mbunda, S. (2020). The impact of provisions on "spreading false information" and "cyberbullying" in Tanzania's Cybercrimes Act on Freedom of expression and democratic engagement. *African Journal of Cyber Law*, 12(1), 98-115.
Misso, P. (2017). The Cybercrimes Act's impact on privacy and freedom of expression in Tanzania: Suppressing dissent due to a lack of judicial oversight. *Tanzanian Journal of Digital Rights and Policy*, 10(2), 156-173.
Mkumbukwa, T. (2019). Ensuring judicial oversight in cybercrime legislation to protect public discourse. *Journal of Legal and Digital Studies*, 12(4), 189-205.
Momen, R. (2019). Internet censorship and its impact on free speech, particularly in political matters. *Middle Eastern Journal of Free Speech*, 7(3), 119-138.
Moyo, T. (2018). Proposing independent bodies to monitor and advocate for changes in cybercrime laws. *Journal of African Governance and Law*, 9(4), 145-162.
Mugarura, H., & Ssali, P. (2021). Judicial oversight by the East African Court of Justice: Balancing security with individual rights in national cybercrime laws. *Journal of East African Studies, 15*(3), 415–432.
Mushi, T. (2020). Judicial oversight and balance in protecting fundamental rights and public discourse.

Journal of Human Rights and Cybersecurity, 15(2), 145-162.
Mwakalebela, J. (2019). Advocating for multi-stakeholder dialogues and regular forums on cybercrime legislation. *Journal of Multi-Stakeholder Policy and Law*, 12(4), 178-195.
Mwangi, W. (2017). Securing against cyber threats without undue speech restrictions: Advocating ongoing legal reform. *Journal of East African Cyber Law*, 8(2), 99-115.
Namuye, K., & Kinuthia, J. (2019). Harmonizing East African cybercrime laws with human rights standards and regional oversight. *East African Journal of Human Rights and Cybersecurity*, 14(2), 87-103.
Ndumbaro, D. D. (2016, February 22nd). *The cyber law and Freedom of expression: The Tanzanian perspectives* Paper]. International Conference, Pretoria. Retrieved July 18th, 2025, from
Nyabola, N. (2018). Stakeholder involvement in crafting East African cybercrime laws: Protecting digital spaces and freedom of expression. *East African Journal of Digital Policy*, 10(2), 77-93.
Nkongho, J. (2016). Africa hosts four of the top ten countries most affected by cybercrime globally. *Journal of African Cybersecurity*, 5(2), 33-49.
Odhiambo, M., & Kamau, J. (2019). Increased surveillance and self-censorship in East Africa. *East African Journal of Cyber Law*, 13(4), 99-115.
Parraguez Kobek, J., & Caldera, E. (2016). Balancing data protection laws and cybersecurity measures: The flexibility of Latin American laws in balancing privacy with law enforcement. *International Journal of Privacy and Cybersecurity*, 8(2), 98-115.
Pollicino, O., & Susi, M. (2019). Surveillance, cybercrime laws, and free speech: A critical analysis. International Journal of Law and Information Technology, 27(1), 56-75. Press.
Popović, D. V. (2021). Freedom of expression on social networks: an international perspective. *The impact of digital platforms and social media on the freedom of expression and pluralism-analysis on certain central European countries. Ferenc Mádl Institute of Comparative Law, Budapest, Hungary*, 277-310.
Quintel, T., & Ullrich, C. (2020). The EU Code of Conduct on Hate Speech: Compatibility with fundamental freedoms. European Law Journal, 26(2), 112-134.
Runa, S. J. (2019). The challenges of Freedom of expression and the Digital Security Act 2018. *BiLD Law Journal*, *4*(2), 75-92.
Sairafi, Z. A. (2022). Cybersecurity Challenges for Human Rights Defenders in Gulf Cooperation Council (GCC) Countries. *Vienna, Austria: Central European University School of Public Policy*.
Schauer, F. (1978). Criticism of the Chilling Effect Theory: Broad and difficult to measure empirically. *Columbia Law Review*, 88(3), 684-726.
Simba, J. (2018). Tanzania's Cybercrime Act and its impact on journalists: Creating a climate of fear. *Tanzanian Journal of Digital Policy*, 14(3), 167-184.
Smith, J. (2018). *Cybercrime legislation and its impact on free speech*. Oxford University
Snail ka Mtuze, S., & Musoni, M. (2023). An overview of cybercrime law in South Africa. *International Cybersecurity Law Review*, *4*(3), 299-323.
Solomon, E. (2022). Cybercrimes Law and Citizen Journalism Clampdown during the Covid-19 Pandemic in Tanzania. *Health Crises and Media Discourses in Sub-Saharan Africa*, 219.
Sombatpoonsiri, J., & Mahapatra, S. (2022). Digital repression during the Covid-19 pandemic in South and Southeast Asia: The impact of laws like Thailand's Computer
Sugow, F., Zalo, E., & Rutenberg, J. (2021). Tensions between enforcing cyber-harassment laws and maintaining free speech in East Africa. *East African Journal of Cyber Law*, 9(3), 112-130.
Swetu, M. (2022). The Position of Electronic and Postal Communication (Online Content) Regulations in Protecting Freedom of Expression in Tanzania. *Available at SSRN 4258336*.

Udoudom, U. (2025). Media ethics and legal reporting in nigeria: balancing freedom of expression and legal constraints in journalism practice. World Journal of Sociology and Law. https://doi.org/10.61784/wjsl3012
Vareba, A. L., Nwinaene, V. P., & Theophilus, S. B. (2017). Internet censorship and freedom of expression in Nigeria. *International Journal of Media, Journalism and Mass Communications, 3*(2), 25-30.
Vese, D. (2022). Governing fake news: The regulation of social media and the right to freedom of

expression in the era of emergency. European Journal of Risk Regulation, 13(2), 17-34. https://doi.org/10.1017/err.2022.1via the internet and digital platforms. *Journal of Digital Law and Security*, 10(2), 87-102.

Wanyeki, M. (2021). Emphasising public consultations and education campaigns for cybercrime legislation. *Journal of Digital Rights and Public Policy*, 17(1), 56-73.

Wiener, F. (1958). The Chilling Effect Theory: Laws and regulations deterring individuals from engaging in legally protected activities. *Harvard Law Review*, 71(5), 679-700.

Zaichuk, O., & Zaichuk, Y. (2019). Freedom of expression, electronic media and cybercrime a rapidly evolving legal landscape. *Yearbook of Ukrainian Law*, *11*, 48.

Ziccardi, G. (2020). Oversight mechanisms and judicial reviews to balance security and freedom of expression: Emphasising transparency. *Global Journal of Digital Policy*, 15(2), 78-96.

Documents

Media Council of Tanzania. (2024). Report on the *State of the media in Tanzania: 2022–2023 report*.

Media Council of Tanzania Legal and Human Rights Centre. (2020). *Tanzania human rights report 2021*. LHRC.

Reporters without Borders. (2024). *World Press Freedom Index 2024*. Tanzania Human Rights Defenders Coalition. (2021). *The situation of human rights defenders in Tanzania: Annual report 2021*. THRDC.

The Cybercrimes Act No. 14, 2015

The CORI Compendium