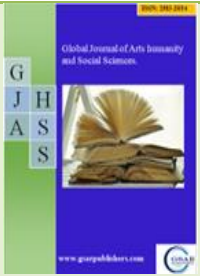


	Global Journal of Arts Humanity and Social Sciences					
	ISSN: 2583-2034					
	Abbreviated key title: Glob.J.Arts.Humanit.Soc.Sci					
	Frequency: Monthly					
	Published By GSAR Publishers					
Journal Homepage Link: https://gsarpublishers.com/journal-gjahss-home/						
Volume - 6		Issue - 10		October 2026	Total pages 929-935	DOI: 10.5281/zenodo.23181388

A CRITICAL ASSESSMENT OF THE LEGISLATIVE PROCESS OF THE CYBERCRIMES ACT, 2015 IN TANZANIA: STAKEHOLDER PARTICIPATION, CONSTITUTIONAL COMPLIANCE AND INSTITUTIONAL CHALLENGES

By

KAAYA, CINDY H.

LL.M Student, St. Augustine University of Tanzania, Mwanza, Tanzania



Article History

Received: 25- 09- 2026

Accepted: 02- 10- 2026

Published: 05- 10- 2026

Corresponding author
KAAYA, CINDY H

Abstract

The rapid development of information and communication technologies has transformed the manner in which individuals, businesses and public institutions communicate and conduct their activities. At the same time, the increased dependence on digital technologies has created new forms of criminal conduct requiring appropriate legal responses. In Tanzania, these developments contributed to the enactment of the Cybercrimes Act, 2015, which provides a legal framework for addressing offences involving computer systems, information and communication technologies. However, the effectiveness and legitimacy of legislation may depend not only on the substantive rules contained in the enacted law but also on the manner in which the legislation is formulated, debated and enacted. This article critically assesses the legislative process that led to the enactment of the Cybercrimes Act, 2015 in Tanzania. It particularly examines stakeholder participation and public consultation, compliance with constitutional and legal principles governing legislative processes, and the procedural and institutional challenges associated with the formulation and enactment of the Act. The article adopts a qualitative legal approach, relying principally on documentary analysis of constitutional provisions, legislation, parliamentary materials, judicial decisions, institutional reports and relevant academic literature. The analysis demonstrates that although the enactment of the Cybercrimes Act, 2015 occurred within the formal parliamentary legislative framework, questions remain concerning the depth of stakeholder participation, the adequacy of consultation and the extent to which technical and rights-related considerations were sufficiently accommodated during the legislative process. The article argues that strengthening participatory mechanisms, technical parliamentary scrutiny and institutional coordination would contribute to more inclusive and constitutionally responsive cyber legislation in Tanzania.

KEYWORDS: Cybercrimes Act, Legislative Process, Public Participation, Constitutional Compliance, Stakeholder Consultation and Cyber Law

1. INTRODUCTION

The development of information and communication technologies has fundamentally changed the manner in which individuals, businesses and public institutions communicate, transact and access information. The increasing reliance on digital systems has, however, been accompanied by new forms of unlawful conduct committed through or directed against computer systems and electronic communications. Cybercrime has consequently become a significant legal concern because its nature differs from

conventional forms of crime in terms of the means through which offences are committed, the location of offenders and victims, and the manner in which electronic evidence is generated and preserved. The growth of these technological developments has therefore placed pressure on States to develop appropriate legal and institutional mechanisms capable of responding to emerging forms of cyber-related criminality.¹

At the international level, cybercrime has increasingly been recognized as a transnational phenomenon requiring legal



responses that extend beyond ordinary domestic criminal law. The United Nations Office on Drugs and Crime has observed the transnational character of cybercrime and the importance of effective legal and institutional mechanisms for its prevention, investigation and prosecution.ⁱⁱ Similarly, the Council of Europe Convention on Cybercrime provides an important international framework for addressing computer-related offences and promoting cooperation between States in the investigation and prosecution of cybercrime. These developments demonstrate that responding to cybercrime is not confined to creating offences and prescribing penalties; it also requires States to develop legislation through processes capable of addressing the technical, legal and human-rights dimensions associated with the regulation of cyberspace.ⁱⁱⁱ

At the African regional level, the increasing use of digital technologies has similarly influenced the development of national and regional legal frameworks dealing with cybersecurity and cybercrime. The African Union Convention on Cyber Security and Personal Data Protection recognizes the need for Member States to establish appropriate legal measures for addressing cybercrime while taking into accounts the protection of fundamental rights. The development of such frameworks illustrates the growing importance of legislation in regulating digital activities. It also raises an important question concerning the manner in which cyber legislation is formulated, particularly where the legislation has the potential to affect rights, impose criminal liability and confer investigative powers upon public authorities.^{iv}

In Tanzania, the expansion of information and communication technologies in social, commercial and governmental activities created a need for a specific legal response to criminal conduct involving computer systems and information and communication technologies. The legislative response culminated in the enactment of the Cybercrimes Act, 2015. The Act was introduced to establish a legal framework for the prevention, investigation and prosecution of cyber-related offences and to address criminal conduct associated with computer systems and electronic communications. The enactment of the legislation represented an important development in Tanzania's legal response to the changing technological environment.^v

Nevertheless, the existence of legislation regulating cybercrime does not, by itself, resolve the question of whether the legislative process through which that law was produced was sufficiently inclusive, constitutionally compliant and institutionally sound. The legitimacy of legislation is closely connected to the process through which it is formulated, scrutinized, debated and enacted. A legislative process provides an opportunity for Parliament, government institutions, professional bodies, civil society and other relevant stakeholders to identify technical difficulties, constitutional concerns and possible consequences arising from proposed legislation. This consideration is particularly important in cybercrime legislation because the subject matter involves specialized technological questions and may affect interests such as freedom of expression, privacy and access to information.^{vi}

The legislative process of the Cybercrimes Act, 2015 has attracted concerns regarding the adequacy of stakeholder participation and public consultation. Available policy and institutional literature had raised questions concerning the extent to which civil society organizations, media stakeholders, legal practitioners and digital-rights actors were adequately involved in the development of the legislation. Such concerns are significant because consultation is not merely a procedural formality. Meaningful participation can provide legislators with information and perspectives that may not otherwise be available within government or parliamentary institutions, particularly where proposed legislation regulates technically complex and rapidly developing areas such as cyberspace.^{vii}

The constitutional dimension of the legislative process is equally important. The Constitution of the United Republic of Tanzania, 1977 establishes the framework within which legislative authority is exercised and provides the broader constitutional foundation for governance and protection of fundamental rights. Consequently, the assessment of the Cybercrimes Act cannot be confined to whether Parliament formally passed the legislation. It is also necessary to consider whether the process through which the legislation was developed and enacted was consistent with the applicable constitutional and legal principles. This becomes particularly relevant where cybercrime legislation intersects with constitutionally protected rights and grants public authorities powers relating to investigation, access to information and electronic communications.^{viii}

Judicial developments have further demonstrated the constitutional significance of cyber-related legislation in Tanzania. Cases such as *Jamii Media Co. Ltd v Attorney General* and *Jebra Kambole v Attorney General* have contributed to judicial consideration of questions involving constitutional rights, legislative authority and the regulation of activities within the digital environment. These developments demonstrate that the relationship between cybercrime regulation and constitutional protection cannot be separated from the broader question of the quality and legitimacy of the legislative framework within which such regulation is established.^{ix}

Apart from stakeholder participation and constitutional considerations, the legislative process may also be affected by procedural and institutional challenges. Cybercrime legislation involves technical issues relating to computer systems, electronic communications, cybersecurity and digital evidence. Effective legislative scrutiny of such matters may therefore require adequate technical expertise and coordination among institutions possessing relevant knowledge. Parliamentary materials and existing literature identified in the research proposal indicate concerns regarding the extent of technical consultation and institutional capacity during the development of cyber-related legislation in Tanzania. The presence or absence of such expertise is relevant because weaknesses at the formulation stage may subsequently affect the clarity, applicability and implementation of legislation.^x

It is against this background that this article critically assesses the legislative process leading to the enactment of the Cybercrimes Act, 2015 in Tanzania. The article focuses on three principal issues: first, the adequacy of stakeholder participation and public consultation; second, the extent to which the legislative process complied with constitutional and legal principles governing law-making; and third, the procedural and institutional challenges that affected the formulation and enactment of the Act. The central concern is therefore not merely whether Tanzania succeeded in enacting legislation dealing with cybercrime, but whether the process through which that legislation was produced provided an adequate foundation for a legitimate, constitutionally responsive and practically workable legal framework.

2. THE LEGISLATIVE PROCESS OF THE CYBERCRIMES ACT, 2015 IN TANZANIA

2.1 Constitutional and Legal Foundation of Legislative Process

The legislative process in Tanzania is founded upon the constitutional allocation of law-making authority and the institutional procedures established for the enactment of legislation. The Constitution of the United Republic of Tanzania, 1977 vests legislative power in Parliament and establishes the constitutional framework within which that power is exercised. The legislative authority of Parliament, however, operates within the wider constitutional order and must therefore be understood together with principles of accountability, constitutionalism and protection of fundamental rights. Law-making consequently involves more than the formal passage of a Bill. It requires consideration of whether the process followed the prescribed legal procedures and whether the resulting legislation remains consistent with the constitutional framework.^{xi}

The constitutional foundation of legislation is particularly important where Parliament is dealing with criminal law. Criminal legislation creates offences, establishes prohibited conduct and may authorize the State to investigate, arrest, prosecute and punish individuals. The legislative process must therefore provide sufficient opportunity for careful examination before criminal liability is imposed. This consideration becomes even more significant in cybercrime legislation because offences involving computer systems and electronic communications often raise technical questions that may not arise in conventional criminal law. The Cybercrimes Act, 2015 therefore required legislative consideration capable of addressing both the criminal-law dimension and the technological environment within which the prohibited conduct occurs.^{xii}

The parliamentary legislative process provides several stages through which a Bill is considered before it becomes law. These stages ordinarily provide opportunities for the proposed legislation to be introduced, debated, examined by the relevant parliamentary committee and considered by Parliament before enactment. In relation to the Cybercrimes Bill, 2015, parliamentary materials indicate that the Bill was subjected to parliamentary consideration

through readings, debate and committee processes. Such procedures are important because parliamentary scrutiny enables proposed provisions to be examined from different perspectives before they acquire binding legal force.^{xiii}

However, formal compliance with parliamentary stages does not necessarily answer every question concerning the quality of the legislative process. A Bill may pass through the required parliamentary stages while questions remain concerning the extent of consultation preceding or accompanying those stages. Parliamentary debate primarily concerns the exercise of legislative authority by elected representatives, whereas public consultation provides an additional opportunity for persons and institutions outside Parliament to contribute specialized knowledge and identify possible consequences of proposed legislation. The distinction is particularly relevant to cybercrime legislation because its application extends beyond government institutions and Parliament to individuals, businesses, technology users, communication providers, media organizations and other actors operating within the digital environment.

The legal foundation of the legislative process must therefore be considered together with the principles governing democratic participation and constitutional governance. Where legislation has the potential to affect fundamental rights, meaningful consideration of those rights during the legislative process becomes an important element of responsible law-making. This is particularly relevant to the Cybercrimes Act, 2015 because certain cybercrime enforcement mechanisms may interact with freedom of expression, privacy and access to information. The subsequent constitutional litigation concerning cyber-related laws illustrates that the relationship between cyber regulation and constitutional rights is not merely theoretical but has generated concrete legal questions before the courts.^{xiv}

The legislative framework must also be considered in light of the wider legal environment governing electronic communications in Tanzania. Before and alongside the Cybercrimes Act, legislation such as the Electronic and Postal Communications Act, 2010 provided an important regulatory framework for electronic communications. The subsequent development of the Personal Data Protection Act, 2022 further demonstrates the continuing expansion of Tanzania's digital legal framework. These law operate within related areas of digital regulation, making institutional and legislative coordination important when developing new legislation. A cybercrime statute therefore cannot be considered in isolation from the broader legal framework governing electronic communications, personal information and digital activities.

2.2 Formulation of the Cybercrimes Bill, 2015

The formulation of the Cybercrimes Bill, 2015 was influenced by the increasing use of information and communication technologies and the emergence of criminal conduct associated with computer systems. The Statement of Objects and Reasons accompanying the Bill provides an important basis for understanding the government's justification for introducing specific legislation addressing cybercrime. The formulation of the Bill reflected the

need to establish offences and corresponding legal mechanisms capable of responding to conduct that could not adequately be addressed through conventional criminal-law provisions alone.^{xv}

The development of the Bill also occurred within an environment in which cybercrime was increasingly understood as a problem requiring specialized legal intervention. Existing studies and institutional reports had drawn attention to the development of cyber-related risks and the need for legal frameworks capable of addressing them. The legislative response was therefore not simply a reaction to individual incidents of cybercrime but formed part of a broader attempt to establish a structured legal framework for cyber-related offences and their investigation.^{xvi}

Nevertheless, the formulation of a cybercrime law presents a particular legislative challenge. The law must be sufficiently precise to satisfy the principle of legality while remaining capable of addressing technological developments that may change rapidly. Overly narrow provisions may become ineffective as technology develops, whereas broadly drafted provisions may create uncertainty concerning the conduct that attracts criminal liability. The formulation stage is therefore an important point at which technical experts, legal professionals, affected institutions and other stakeholders can identify potential difficulties in proposed provisions before enactment.

This consideration gives practical significance to the question of stakeholder participation. Where a proposed law regulates a specialized field, consultation can provide access to knowledge that may not be available within the ordinary legislative process. In the context of cybercrime, such knowledge may relate to information technology, electronic evidence, telecommunications, data protection, media practice, criminal investigation and constitutional rights. Literature concerning Tanzania's cyber regulatory environment has raised concerns regarding limited stakeholder involvement during the development of cyber legislation, particularly in relation to civil society and digital-rights stakeholders.^{xvii}

The formulation process should therefore be assessed not only by reference to whether the Government prepared and introduced a Bill, but also by considering whether the process created adequate opportunities for relevant interests to contribute to the content of the proposed legislation. This distinction is important because the quality of a legislative process may be affected by the range and depth of information available to those responsible for drafting and scrutinizing the proposed law.

2.3 Parliamentary Consideration and Enactment

Following its formulation, the Cybercrimes Bill proceeded through the parliamentary process before becoming the Cybercrimes Act, 2015. Parliamentary records, including Hansard debates and committee materials, provide documentary evidence of the consideration given to the Bill during its passage through Parliament. These materials are important sources for assessing not only the formal progression of the Bill but also the issues that were raised, discussed and considered during parliamentary deliberations.^{xviii}

Parliamentary consideration serves an important constitutional function because it provides the principal institutional forum through which proposed legislation is examined before enactment. Debate allows Members of Parliament to question the necessity, content and possible consequences of proposed provisions, while committee scrutiny provides an opportunity for more detailed consideration of the Bill. In a specialized field such as cybercrime, the effectiveness of this process depends partly on the availability of adequate legal and technical information to support parliamentary examination.

The parliamentary record should therefore be examined alongside other documentary materials rather than treated as conclusive evidence of comprehensive stakeholder participation. The existence of parliamentary debate establishes that representatives considered the Bill, but it does not necessarily establish the extent to which persons outside Parliament were consulted during its formulation. This distinction is central to assessing the legislative process because parliamentary participation and public consultation perform related but different functions. The available literature has raised concerns that the legislative process surrounding Tanzania's cybercrime framework involved limited engagement with certain stakeholders, including civil society organizations and digital-rights actors. At the same time, parliamentary records demonstrate that the Bill was subjected to formal parliamentary procedures. The issue is therefore not simply whether the Bill was legally presented and passed through Parliament, but whether the formal process was sufficiently complemented by meaningful consultation and technical engagement.^{xix}

The enactment of the Cybercrimes Act, 2015 consequently marked an important stage in the development of Tanzania's cyber legal framework. The Act established offences and legal mechanisms directed towards cyber-related criminal conduct, thereby providing a specific statutory basis for addressing conduct involving computer systems and information and communication technologies. Nevertheless, the circumstances surrounding its formulation and enactment remain relevant when assessing the legitimacy, responsiveness and practical adequacy of the legislative framework.^{xx}

3. STAKEHOLDER PARTICIPATION AND PUBLIC CONSULTATION

Stakeholder participation is an important part of legislative development because it allows persons and institutions affected by proposed legislation to present their views before the law is enacted. This is particularly important in cybercrime legislation because the subject involves criminal law, technology, electronic communications and fundamental rights.^{xxi} The Cybercrimes Bill, 2015 was formally published before its consideration by Parliament, together with its Statement of Objects and Reasons. However, publication of a Bill does not necessarily amount to meaningful public consultation. Contemporary assessments raised concerns that civil society organizations and other relevant stakeholders had limited involvement in the formulation of the Bill.

This raises an important distinction between making a Bill publicly available and providing an effective opportunity for stakeholders to influence its development.^{xxii}

The concern is significant because the Cybercrimes Act regulates matters requiring specialized knowledge, including computer-related offences, electronic evidence and investigative powers. Involving ICT experts, legal practitioners, media stakeholders and civil society could therefore assist in identifying technical difficulties and possible implications for fundamental rights before enactment.^{xxiii} The parliamentary process nevertheless provided an institutional opportunity for debate and scrutiny of the Bill. Parliamentary records show that the Bill proceeded through the formal legislative process before becoming law. However, formal parliamentary consideration does not, by itself, establish that adequate consultation occurred outside Parliament. Public participation and parliamentary debate perform different functions: Parliament exercises legislative authority, while consultation provides additional information and perspectives from affected sectors.^{xxiv}

The issue became more significant following the enactment of the Act, as concerns were raised regarding freedom of expression, privacy and investigative powers. These concerns subsequently became subjects of constitutional litigation, including challenges concerning sections 32 and 38 of the Act. Although the High Court upheld the challenged provisions, the litigation demonstrates the importance of considering rights-related concerns during the legislative stage. Therefore, the available material suggests that the legislative process formally complied with parliamentary requirements, but questions remain regarding the depth and inclusiveness of stakeholder consultation. The issue is not whether every stakeholder proposal should have been accepted, but whether relevant stakeholders were given a genuine and timely opportunity to contribute before the legislation was enacted.^{xxv}

4. CONSTITUTIONAL AND LEGAL COMPLIANCE IN THE LEGISLATIVE PROCESS

4.1 Constitutional Requirements Governing Law-Making

The legislative process of the Cybercrimes Act, 2015 must be examined against the constitutional framework governing the making of laws in Tanzania. The Constitution vests legislative power in Parliament and establishes procedures through which Bills are introduced, debated and enacted. The constitutional framework therefore requires legislation to derive its validity not only from its substantive content but also from compliance with the prescribed legislative procedure.^{xxvi} In the case of the Cybercrimes Act, 2015, the Bill was introduced before Parliament and subjected to parliamentary debate before receiving presidential assent. The parliamentary record therefore indicates compliance with the formal stages of legislative enactment. However, formal compliance should be distinguished from the broader constitutional principles of participation, accountability and protection of fundamental rights.^{xxvii}

4.2 Compliance with Parliamentary Legislative Procedures

The legislative process involved publication of the Cybercrimes Bill, parliamentary consideration and subsequent enactment. The Statement of Objects and Reasons identified the principal purpose of the proposed legislation, including the creation of offences relating to computer systems and electronic communications and the establishment of mechanisms for investigation and prosecution.^{xxviii} Nevertheless, compliance with parliamentary procedure does not necessarily establish that every stage of policy formulation was sufficiently consultative. The legislative record is therefore important in determining whether parliamentary scrutiny adequately considered the technical, social and constitutional implications of the proposed offences and investigative powers.^{xxix}

4.3 Protection of Fundamental Rights

A further issue concerns the compatibility of the legislative process and resulting legislation with constitutional rights. The Cybercrimes Act regulates conduct occurring in the digital environment, but several of its provisions affect interests such as freedom of expression, privacy and access to information. The Constitution protects these interests while permitting limitations prescribed by law and subject to constitutional requirements.^{xxx} The subsequent constitutional challenges to provisions of the Act demonstrate the importance of examining fundamental rights during the legislative process itself. In *Jamii Media Co. Ltd v Attorney General*, the High Court considered challenges concerning provisions of the Act, illustrating how questions that may arise during legislative scrutiny can later become matters for judicial determination.^{xxxi}

4.4 Judicial Scrutiny of the Cybercrimes Act

Judicial review provides an important mechanism for testing whether legislation conforms to constitutional requirements. The litigation concerning the Cybercrimes Act shows that enactment by Parliament does not place legislation beyond constitutional scrutiny. The significance of this is that legislative effectiveness should not be assessed solely by the speed or completion of enactment, but also by whether the process and resulting law sufficiently accommodate constitutional rights and legal safeguards. Accordingly, the legislative process leading to the Cybercrimes Act, 2015 demonstrates substantial formal parliamentary compliance, but questions remain concerning the depth of constitutional and rights-based scrutiny during its formulation. This distinction is central to assessing the effectiveness of the legislative process rather than merely confirming that the Act was formally enacted.

5. PROCEDURAL AND INSTITUTIONAL CHALLENGES IN THE LEGISLATIVE PROCESS

5.1 Limited Stakeholder Participation

One of the principal challenges concerns the extent to which stakeholders were involved before the Cybercrimes Bill was enacted. Although the Bill was formally introduced and debated in Parliament, the available literature raises questions about whether consultation outside Parliament was sufficiently broad and

meaningful. This is particularly important because cybercrime legislation affects lawyers, technology professionals, media practitioners, private businesses, civil society and ordinary users of digital services. The absence of sufficiently inclusive consultation may limit the opportunity to identify technical difficulties and potential effects on fundamental rights before enactment.

5.2 Technical Complexity of Cybercrime Legislation

Cybercrime legislation presents a further challenge because of the technical nature of the subject. Effective law-making in this area requires an understanding of computer systems, electronic evidence, digital investigations and emerging forms of criminal conduct. Where legislative formulation is not adequately informed by technical expertise, there is a risk of adopting provisions that are difficult to interpret or apply in practice. The legislative process therefore requires cooperation between legal institutions and relevant technological stakeholders.

5.3 Institutional Coordination

The formulation and implementation of cybercrime legislation also involve several institutions, including Parliament, law-enforcement agencies, the judiciary, the Tanzania Communications Regulatory Authority and other bodies responsible for information and communications technology. Effective legislation consequently depends not only on the wording of the Act but also on coordination among institutions responsible for its enforcement. Institutional fragmentation may create difficulties in determining responsibilities, developing technical capacity and ensuring consistent application of the law.

5.4 Tension Between Cybersecurity and Fundamental Rights

Another significant challenge is maintaining an appropriate balance between combating cybercrime and protecting constitutional rights. Some provisions of the Cybercrimes Act have attracted legal and human-rights concerns, particularly in relation to freedom of expression, privacy and access to information. The subsequent constitutional litigation concerning provisions of the Act demonstrates that these concerns cannot be separated from the quality of the legislative process. A more comprehensive assessment of rights implications at the formulation stage could assist in reducing later legal uncertainty and constitutional challenges.

5.5 Limited Legislative Responsiveness to Technological Change

Technology develops considerably faster than conventional legislative processes. Consequently, legislation enacted to address particular forms of cybercrime may encounter new technological practices that were not anticipated during its formulation. This creates a continuing need for legislative review, institutional capacity-building and consultation with technical experts. The effectiveness of the Cybercrimes Act therefore depends not only on its original legislative process but also on the ability of the legal and institutional framework to respond to subsequent technological developments.

6. RECOMMENDATIONS

Based on the assessment of the legislative process leading to the enactment of the Cybercrimes Act, 2015, the following measures are recommended:

First, stakeholder consultation should be strengthened in the formulation of cybercrime legislation. Future Bills should provide adequate opportunities for ICT professionals, legal practitioners, media organizations, civil society and other affected stakeholders to submit views before parliamentary consideration.

Second, technical expertise should be incorporated into the legislative process. Parliament and relevant government institutions should engage ICT and cybersecurity specialists when formulating or reviewing cybercrime legislation so that proposed provisions correspond with technological realities.

Third, constitutional and human-rights assessment should form part of the legislative process. Proposed cybercrime provisions should be examined against constitutional rights, particularly freedom of expression, privacy and access to information, before enactment. This may reduce subsequent uncertainty and constitutional litigation.

Fourth, institutional coordination should be improved. Institutions involved in the investigation, prosecution, adjudication and regulation of cybercrime should have clearly defined responsibilities and adequate technical capacity to implement the legislation effectively.

Fifth, the Cybercrimes Act should be periodically reviewed to respond to technological developments and emerging forms of cybercrime. Regular legislative review would allow Parliament to identify provisions that have become inadequate, unclear or difficult to apply in light of changes in technology.

7. CONCLUSION

The assessment of the legislative process leading to the enactment of the Cybercrimes Act, 2015 shows that Tanzania established a statutory framework intended to address cybercrime and regulate criminal conduct involving information and communication technologies. Although the Bill underwent the formal parliamentary process and was enacted into law, the assessment reveals that formal compliance with parliamentary procedures alone does not necessarily demonstrate a fully satisfactory legislative process. Particular concerns arise regarding the extent of stakeholder participation, public consultation, technical expertise and consideration of constitutional rights during the formulation of the legislation. The subsequent legal challenges concerning certain provisions of the Act further demonstrate the importance of incorporating constitutional and human-rights considerations at the legislative stage. The study therefore concludes that an effective legislative process for cybercrime legislation requires meaningful stakeholder participation, adequate technical expertise, constitutional scrutiny and effective institutional coordination to ensure that the resulting legal framework responds to technological developments while remaining consistent with constitutional principles.

END NOTES

- ⁱ Collaboration on International ICT Policy for East and Southern Africa (CIPESA) (2016), State of Internet Freedom in Tanzania; ARTICLE 19 Eastern Africa (2015), Tanzania: Freedom of Expression and Digital Rights in the Cybercrimes Act, 2015.
- ⁱⁱ United Nations Office on Drugs and Crime (UNODC) (2013), Comprehensive Study on Cybercrime.
- ⁱⁱⁱ Council of Europe (2001), Convention on Cybercrime (Budapest Convention).
- ^{iv} African Union (2014), African Union Convention on Cyber Security and Personal Data Protection.
- ^v United Republic of Tanzania (2015), The Cybercrimes Act, No. 14 of 2015.
- ^{vi} Article 19 Eastern Africa (2015), Analysis of Tanzania's Cybercrimes Act; see also African Commission on Human and Peoples' Rights (2019), Declaration of Principles on Freedom of Expression and Access to Information in Africa.
- ^{vii} CIPESA (2016), State of Internet Freedom in Tanzania; Article 19 Eastern Africa (2015), Analysis of Tanzania's Cybercrimes Act.
- ^{viii} Constitution of the United Republic of Tanzania, 1977 (as amended).
- ^{ix} Ibid.
- ^x Parliament of the United Republic of Tanzania (2015), Hansard Debates on the Cybercrimes Bill, 2015.
- ^{xi} Constitution of the United Republic of Tanzania, 1977 (as amended).
- ^{xii} United Republic of Tanzania, The Cybercrimes Act, No. 14 of 2015.
- ^{xiii} Ibid.
- ^{xiv} Ibid.
- ^{xv} Ibid.
- ^{xvi} United Nations Office on Drugs and Crime (UNODC) (2013), Comprehensive Study on Cybercrime; Council of Europe (2001), Convention on Cybercrime.
- ^{xvii} Collaboration on International ICT Policy for East and Southern Africa (CIPESA) (2016), State of Internet Freedom in Tanzania; Article 19 Eastern Africa (2015), Analysis of Tanzania's Cybercrimes Act.
- ^{xviii} Parliament of the United Republic of Tanzania, Hansard Debates on the Cybercrimes Bill, 2015; Parliament of the United Republic of Tanzania, Report of the Parliamentary Standing Committee on the Cybercrimes Bill, 2015.
- ^{xix} CIPESA (2016), State of Internet Freedom in Tanzania; Article 19 Eastern Africa (2015), Analysis of Tanzania's Cybercrimes Act.
- ^{xx} United Republic of Tanzania, The Cybercrimes Act, No. 14 of 2015.
- ^{xxi} African Commission on Human and Peoples' Rights, Declaration of Principles on Freedom of Expression and Access to Information in Africa (2019).
- ^{xxii} Global Integrity, Opening Government? Tanzania Final Report (2018).

^{xxiii} Ibid.

^{xxiv} Parliament of the United Republic of Tanzania, Hansard Debates on the Cybercrimes Bill, 2015; Report of the Parliamentary Standing Committee on the Cybercrimes Bill, 2015.

^{xxv} Ibid.

^{xxvi} Constitution of the United Republic of Tanzania, 1977, Article 62-98.

^{xxvii} Parliament of the United Republic of Tanzania, Hansard Debates on the Cybercrimes Bill, 2015.

^{xxviii} United Republic of Tanzania, The Cybercrimes Bill, 2015, Bill Supplement No. 4, 20 February 2015.

^{xxix} Parliament of the United Republic of Tanzania, Report of the Parliamentary Standing Committee on the Cybercrimes Bill, 2015.

^{xxx} Constitution of the United Republic of Tanzania, 1977, Article. 18, 21 and 30.

^{xxxi} Ibid.