International Journal of Economics, Commerce and Management
United Kingdom ISSN 2348 0386 Vol. 14, Issue 2, Feb 2026

https://ijecm.co.uk/

APPLICATION OF E-COMMERCE LAW IN TANZANIA AND CONSUMER PROTECTION: A LEGAL PARADOX

Khadija Abdalla Amour
Dar Es Salaam Maritime Institute, Tanzania
ummunoordin8417@outlook.com

Tumaini S Gurumo
Dar Es Salaam Maritime Institute, Tanzania
tgurumo@gmail.com

Abstract

This article assesses Tanzania's e-commerce legal framework and consumer protection by examining the Electronic Transactions Act, Cap 442 R.E. 2023, the Fair Competition Act of 2024, the Cybercrimes Act No. 14 of 2015, and the Personal Data Protection Act No. 11 of 2022. In order to lead Tanzania's digital economy, this article assesses how well these laws protect online consumers, assesses the coherence of the legal framework, analyses regulatory bodies' enforcement and implementation efforts, and identifies best practices from benchmark nations. The study uses a qualitative doctrinal and comparative legal methodology based on statutory analysis, policy documents, judicial decisions, and secondary literature, supported by insights drawn from the EU's General Data Protection Regulation (GDPR) and Kenya's Data Protection Act, 2019. As per the findings, Tanzania has made progress but there are still significant gaps. There are insufficient enforcement procedures. Mandates for regulations overlap. There are disparate legal provisions. Low public knowledge and the lack of a single e-commerce policy further restrict consumer rights online. The situation is made worse by practical issues such low institutional capacity, cross-border fraud, and jurisdictional difficulties. The article recommends stronger institutional coordination, harmonised laws, improved capacity-building for enforcement agencies, greater consumer awareness, and enhanced regional cooperation within the East African Community.

Keywords: e-commerce, consumer protection, platform liability, legal paradoxes, personal data protection

INTRODUCTION

The rising influence of digital technologies on commercial transactions has affected both the dynamics of customer interactions and global trade. In Tanzania, e-commerce the buying and selling of goods and services through online platforms has grown quickly, opening up new possibilities for productivity, creativity, and inclusivity in both urban and rural marketplaces. In this sense, “consumer rights” refers to the safeguards and assurances that guarantee secure, equitable, and transparent online transactions, such as the right to accurate information, privacy, safe payments, and efficient channels for recourse. Enforcing these safeguards through legislative frameworks and regulatory supervision is part of the implementation of e-commerce consumer rights law. The problem at the heart of this article, however, is that consumers are still susceptible to fraud, false information, privacy violations, and inadequate dispute resolution procedures despite progressive laws like the Electronic Transactions Act, Cap 442 R.E. 2023, the Fair Competition Act No. 13 of 2024, the Cybercrime Act No. 14 of 2015, and the Personal Data Protection Act No. 11 of 2022. In order to improve Tanzania’s consumer protection in e-commerce, this article evaluates the effectiveness of these laws in protecting online consumers, evaluates the consistency of the legislative framework, examines the enforcement and implementation efforts of regulatory authorities, and identifies best practices from benchmark countries.

LITERATURE REVIEW

There has been significant progress in acknowledging consumer rights in the digital domain, as seen by the expanding body of research on Tanzanian e-commerce and consumer protection. Tanzania has passed a number of laws controlling digital transactions, but substantive consumer protection is still scarce and unevenly applied, according to research on e-commerce regulation in the nation. Scholarly research indicates that consumer rights are becoming more widely acknowledged in the digital marketplace, yet there are still large discrepancies between legal guarantees and real customer experiences. While emphasising the unique contribution of the current study, this review summarises pertinent research on substantive legal adequacy, regulatory coherence, enforcement capacity, and comparative best practices.

Substantive Adequacy of Tanzania’s Consumer Protection Laws

Whether Tanzanian laws offer adequate substantive protections for internet consumers is a central subject in the research. According to Mwasomola (2020), the Electronic Transactions Act, Cap 442, R.E. 2023, validates electronic signatures and contracts but is

primarily procedural in nature, missing cooling-off periods, statutory disclosure requirements, and protections against deceptive online operations. Customers are seriously vulnerable as a result of these omissions. Building on this study, the current article demonstrates how these significant gaps expose consumers to information asymmetries and deceptive digital marketing, and it suggests specific changes for improved online consumer rights.

Tanzania's e-commerce law needs clear anti-fraud provisions, transparency requirements, and thorough distance-selling restrictions, according to earlier foundational work by Mambi (2015; 2019). His analysis is still relevant, but it requires sufficient institutional capacity to uphold such standards. The current study expands Mambi's work by showing how weak enforcement mechanisms and growing regulatory complexity have hindered the implementation of these reforms. It contends that in order to accomplish significant consumer protection, institutional capacity must be improved in tandem with legislative reform.

The concept of the "electronic consumer" is introduced by Mwenegoha (2015), who emphasises that existing consumer protection mechanisms created for physical marketplaces are insufficient for digital contexts. Additionally, he cautions that implementing foreign legal models without making necessary contextual adjustments could result in poor regulatory outcomes. By connecting consumer vulnerability to more recent threats like data privacy violations, algorithmic manipulation, and platform dominance areas where Tanzanian law is still in its infancy this study upholds and expands on that stance.

International perspectives also enrich the understanding of consumer vulnerability in digital markets. Agibalova, Ivanova, and Petrov (2020) argue that digitalisation has increased the risk of deceptive pricing, data misuse, and algorithm-driven unfair practices globally. Applying these insights to Tanzania, the present article highlights the absence of legal responses to these emerging risks and demonstrates how global digital harms manifest within the Tanzanian regulatory framework.

Coherence and Fragmentation of the Legal Framework

Significant fragmentation is shown by literature on Tanzania's digital regulatory framework's coherence. Kaukab (2025) emphasises that in order to accommodate digital marketplaces, emerging nations must update and unify their consumer protection legislation. This article applies this concept to Tanzania and shows how the Personal Data Protection Act of 2022, the Electronic Transactions Act, and the Fair Competition Act of 2024 are inconsistent. These discrepancies erode consumer confidence and make the law less predictable.

According to Bartosz's (2020) analysis of international e-commerce systems, regulatory harmonisation is essential for effective digital markets. This essay applies this understanding to

East Africa and demonstrates how Tanzania's sector-based mandates and overlapping rules make it difficult to implement regulations coherently and comply with the frameworks of the African Continental Free Trade Area (AfCFTA) and East African Community (EAC).

According to Harvey and King (2022), transnational hazards in e-commerce include limited redress procedures, ambiguous platform liability, and unclear jurisdiction. These insights show that Tanzanian laws do not sufficiently manage cross-border disputes and the accountability of foreign-based platforms. By evaluating the effects of lax cross-border enforcement on Tanzanian consumers, the current paper broadens this criticism.

Enforcement, Institutional Capacity, and Implementation

The effectiveness of enforcement and institutional preparedness constitute another important body of knowledge. Oreku (2013) emphasises that without technological capability, administrative expertise, and public digital literacy, e-commerce law reforms cannot be successful. These difficulties continue, according to recent national statistics. This article extends Oreku's findings by demonstrating that, in spite of legal revisions, enforcement is still inadequate because of conflicting institutional missions, tight budgets, and a lack of human resources.

Anwar, Samsudin, and Harry's (2021) analysis of comparative data from Indonesia shows how weak enforcement and disjointed regulatory frameworks compromise consumer protection in digital markets. This article suggests the creation of a dedicated digital consumer protection body and draws comparisons with Tanzania, pointing out similar shortcomings, especially redundancy across institutions like the TCRA, FCC, and Bank of Tanzania.

Kangole's empirical research on Tanzania's financial technology ecosystem reveals that institutions frequently lack the capacity to handle digital complaints and that current regulatory processes do not sufficiently protect customers using mobile and internet banking. His findings are extended to non-financial e-commerce platforms in this research, demonstrating the persistence of comparable enforcement gaps among digital service providers and online marketplaces.

A healthy digital economy is built on consumer trust, which is dependent on robust enforcement, according to UNCTAD (2020) and economist Honest Ngowi. They point out that coordination between regulatory agencies is hampered by Tanzania's absence of a national e-commerce policy. By showing how uneven enforcement erodes digital trust, deters market participation, and delays the expansion of Tanzania's digital economy, the current study expands on this analysis.

Comparative Best Practices and Regional Insights

The importance of comparative frameworks in enhancing e-commerce regulation is well acknowledged in the literature. In order to address cross-border digital consumer issues, Riefa's (2019) UNCTAD paper emphasises the significance of harmonised norms, extraterritorial enforcement, and mutual legal support. By suggesting region-specific changes for the EAC and AfCFTA, such as cross-border enforcement databases and coordinated dispute resolution procedures, this article builds on her suggestions.

According to George and Simi (2019), consumer protection regimes must be modified on a regular basis to accommodate digital innovation. According to their comparative research, online participation is higher in jurisdictions with robust platform accountability, thorough consumer education, and well-thought-out digital market planning. The current paper applies this to Tanzania, identifying gaps in consumer awareness programs and suggesting focused interventions to improve platform obligations and boost digital literacy.

Manteaw (2020) points out flaws in Ghana's consumer protection and e-commerce laws, such as deficiencies in electronic contracting and fraud prevention. In order to show that Tanzania may implement Ghana's reforms on legislative harmonisation, oversight of electronic payments, and institutional development, the current study uses these findings as a benchmark for Tanzania.

Abdullah, Alshatebi, Bouke, and associates (2023) examine Africa's regional cybersecurity and data protection framework in accordance with the AU Malabo Convention at the continental level. They draw attention to inadequate institutional networks, capability limitations, and inconsistent legal frameworks among member nations. Building on previous findings, the current study makes the case for more robust regional cooperation and stricter enforcement of the Personal Data Protection Act 2022 to guarantee uniform implementation of digital rights regulations.

METHODOLOGY

The Study

The article assesses Tanzania's e-commerce and consumer protection framework using a qualitative, desk-based methodology and a doctrinal legal research design. This article evaluates the Tanzania's e-commerce laws and consumer protection system using a qualitative doctrinal and comparative legal methodology.

Research Design and Approach

The article uses a qualitative, desk-based methodology with a doctrinal legal research design. This describes the general framework of the research, which focusses on analysing legal principles by looking at laws, statutes, regulations, and case law.

The Electronic Transactions Act, Cap 442 R.E. 2023, the Cybercrimes Act No. 14 of 2015, the Fair Competition Act No. 13 of 2024, the Personal Data Protection Act No. 11 of 2022, and TCRA regulations are among the key sources that are examined. Additionally examined are records from organisations like the Police Force and the Fair Competition Commission, as well as case law from Tanzanian courts. These resources offer a starting point for evaluating Tanzania's e-commerce and consumer protection legislation.

Academic literature, policy documents, and institutional reports obtained from reliable online databases and libraries such as the University of Dar es Salaam, the High Court, and the Attorney General's Chambers are used as secondary sources. Legal gaps, overlaps, and enforcement issues are found using content and theme analysis. Benchmarks are provided via comparative analysis of the GDPR, the Data Protection Act of Kenya, and the Consumer Protection Act of South Africa. This method enables the study to assess Tanzania's consumer protection and e-commerce legislation' practical efficacy as well as their sufficiency.

Study Area

The proposed study will be conducted in Dar Es Salaam which is the metropolis and economic centre. It is home to important financial institutions, regulatory bodies, and technology service providers as the hub of the nation's digital economy. Additionally, the city contains Tanzania's largest concentration of digital customers, e-commerce companies, and internet users. The study's focus on Dar es Salaam enables it to document the institutional, legal, and practical aspects of consumer protection and e-commerce in the nation's busiest online market.

Data Analysis and Interpretation

The collected data will be analysed using documentary content analysis. Key words, phrases, and legal provisions from statutes, case law, regulatory documents, and policy papers will be coded and categorised into themes. Interpretation will employ both literal and purposive approaches to statutory interpretation, while inductive legal reasoning will guide the evaluation of patterns and relationships. Findings will be aligned with the study's objectives and research questions. A database will be maintained for systematic storage, reference, and verification of extracted data.

FINDINGS

Effectiveness of E-Commerce Laws in Safeguarding Consumers

The Tanzania's e-commerce regulations, which are based on the Electronic Transactions Act (ETA), Cap 442 R.E. 2023, the Fair Competition Act No. 13 of 2024, the Cybercrimes Act No. 14 of 2015, and the Personal Data Protection Act (PDPA) No. 11 of 2022, provide a wide range of rights to protect online shoppers. These laws, in theory, provide procedures for redress, honest commercial interactions, safe electronic transactions, and personal data protection. However, national reports, enforcement patterns, and court rulings demonstrate that consumers' practical protection is still restricted, exposing a persistent legal conundrum. Baseline protections are provided by the Electronic Transactions Act (ETA), Cap 442 R.E. 2023, which mandates secure electronic recordkeeping and authentication processes in addition to requiring online vendors to publish accurate information about items, prices, identification, and terms of sale. It represents systemic flaws in electronic authentication and consumer protections typical of online marketplaces, even though it isn't technically an e-commerce issue. In a similar vein, the Fair Competition Commission (FCC) has frequently documented instances of deceptive online marketing and fake items sold on social media platforms, suggesting that the FCA's rules regarding unfair commercial practices are not adequately implemented in digital settings.

Enhancing data protection in accordance with worldwide standards is the goal of the Personal Data Protection Act (PDPA) No. 11 of 2022. It clearly requires data controllers and processors to manage personal data in a way that complies with the law. Nonetheless, widespread non-compliance among digital platforms is reported by the Tanzania Communications Regulatory Authority (TCRA). Weak consent procedures, disregard for data-retention restrictions, and tardiness in breach reporting are common infractions. Implementation issues are further highlighted by high-profile examples of fraudulent SIM card registration and illegal data sharing. These regulations are supported by the Cybercrimes Act No. 14 of 2015, which makes identity theft, internet fraud, and unauthorised access illegal. However, rather than addressing more general flaws in platform security or consumer-redress procedures, it frequently targets specific offenders.

There are ongoing structural issues, according to reports from the Ministry of Information, Communication, and Information Technology, the Fair Competition Commission (FCC), and TCRA. These include poor regulatory cooperation, insufficient digital forensics capabilities, and restricted institutional capability. Because of this, authorities find it difficult to keep an eye on online marketplaces, handle complaints about cross-border e-commerce, or impose fines on non-compliant service providers. Additionally, public awareness is poor,

especially in rural areas. Many customers fail to disclose data breaches or seek remedies, which makes enforcement even weaker and permits recurrent infractions. The consumer experience is nonetheless precarious despite the overall strength of the legal system. The legal dilemma is centred on this disparity. Tanzania has up-to-date, internationally compliant regulations pertaining to cybersecurity, data protection, and consumer protection. However, their effectiveness is weakened by inadequate enforcement, a lack of capacity, and poor public awareness. As a result, even with extensive legislation, consumers still have to deal with internet fraud, misleading advertising, and privacy intrusions. On paper, the system functions well, but in reality, it performs terribly. To bridge the gap between legislative protections and real consumer safety in Tanzania's e-commerce industry, stronger enforcement, better regulatory coordination, enhanced public education, and increased technical investment are required.

The High Court acknowledged the legality of using electronic communications to create contracts in *Paulo Samson v. Serena Hotel* Commercial Case No. 76 of 2018 (High Court of Tanzania, Commercial Division). This bolsters the claim that electronic contracts are accepted by the ETA. However, consumers are still at danger of receiving false or misleading information from the internet. The case demonstrates that companies have an obligation to offer trustworthy digital content, which is essential to protecting consumers. The Court of Appeal affirms the admissibility of electronic documents as evidence in *Stanbic Bank Tanzania Ltd v Tanzania Revenue Authority,* Civil Appeal No. 57 of 2017 (Court of Appeal of Tanzania) . This shows that rights resulting from digital exchanges can be enforced by courts. But it also reveals a dilemma. Although the legislation encourages digital transactions, disagreements persist because many electronic systems lack consumer protection and transparency.

Cohesion and Implementation of the Legal Framework

Tanzania's e-commerce legal framework appears comprehensive in design, yet its cohesion and implementation remain weak due to fragmentation, overlapping mandates, and inconsistent enforcement. Reports by the Tanzania Communications Regulatory Authority (TCRA) consistently show that major compliance failures persist among digital platforms. For example, TCRA's Q4 2022 Communications Statistics Report records 12,613 fraudulent SIM-card practices and 2,969 consumer complaints within a single quarter, exposing widespread weaknesses in identity verification, data-handling, and consumer-protection practices. In its 2024 enforcement updates, TCRA further reports the deactivation of 12,896 fraudulent SIM cards, illustrating both the magnitude of cyber-fraud risks and the limited preventative capacity of regulators. These enforcement issues are made worse by the fragmentation of regulatory

authority. Although their responsibilities often overlap, the Fair Competition Commission (FCC), TCRA, and the recently formed Personal Data Protection Commission (PDPC) are all in charge of consumer protection, digital markets, and data privacy. The Tanzania Digitalisation Journey report from GSMA attests to the continued lack of institutional coordination, with regulators frequently operating independently rather than together. Similar gaps in digital-forensics resources, inter-agency information sharing, and monitoring capability are noted by the Ministry of Information, Communication, and Information Technology. These gaps make it difficult to apply the Electronic Transactions Act, the Fair Competition Act, and the Personal Data Protection Act (PDPA) No. 11 of 2022 consistently across online marketplaces.

Implementing data protection poses extra difficulties. Although the Personal Data Protection Act (PDPA) No. 11 of 2022 has been in effect since 2022, many mobile network operators fail to adequately disclose their biometric-data practices upon SIM registration, resulting in privacy concerns, according to the Digital Agenda Initiative Report. The report also notes that early on in its implementation, the PDPC was not entirely operational, which led to confusion over compliance and delayed enforcement preparedness. The State of Internet Governance Report 2024 and the Tanzania Digital Rights Index 2024 support these conclusions by highlighting persistent data-privacy issues, illegal data sharing, and inadequate complaint-resolution procedures. All of these evaluations demonstrate that while the the Personal Data Protection Act (PDPA) No. 11 of 2022 offers robust legal protections, public awareness and actual enforcement fall well short.

There is little direction from judicial practice to improve coherence within the framework. Tanzania has extremely few determined cases pertaining to the Electronic Transactions Act or the Personal Data Protection Act (PDPA) No. 11 of 2022, indicating that either enforcement does not proceed to litigation or that consumers lack the information or confidence to seek remedies. Due to a lack of knowledge about digital rights, many consumers especially in rural areas do not report online fraud, misleading digital behaviour, or privacy violations. This disparity reflects the larger reality disclosed by FCC and TCRA reports.

When combined, the legitimate institutional reports demonstrate that Tanzania's e-commerce regulations are still robust in theory but operate poorly in reality. The efficacy of the regulatory structure is compromised by overlapping mandates, poor coordination, a lack of digital forensics capabilities, and low public awareness. Because of this, the legal system operates in a fragmented and reactive fashion, and despite the existence of contemporary laws meant to protect them, consumers still face serious risks, such as fraud, dishonest online behaviours, and privacy violations. The fundamental legal contradiction in Tanzania's e-commerce ecosystem is this discrepancy between statutory design and actual consumer experience.

Lessons from Benchmark Jurisdictions

Leading countries' comparative observations offer insightful recommendations for enhancing consumer safety in Tanzania's e-commerce sector. Through stringent permission requirements, required breach notifications, and severe fines for non-compliance, the General Data Protection Regulation (GDPR) of the European Union exemplifies how a complete, rights-based data governance approach increases consumer trust in digital transactions. This approach demonstrates that, in contrast to Tanzania's existing more dispersed enforcement procedures, defined rights and credible consequences produce higher deterrence and responsibility.

Kenya's Data Protection Act, 2019 provides a significant regional benchmark because of its comparable socioeconomic setting. Kenya operationalises its laws through the appointment of an independent Data Protection Commissioner, who has the specific power to establish sector standards, levy administrative penalties, and carry out extensive public awareness campaigns. In contrast to Tanzania's fragmented institutional systems, this centralised supervision model demonstrates how precise regulatory mandates and organised complaint-handling processes can enhance compliance among digital service providers.

The Protection of Personal Information Act (POPIA) and South Africa's Consumer Protection Act, 2008 both emphasise how important it is to include data privacy and consumer justice into a logical regulatory framework. These laws place a strong emphasis on statutory provider requirements, straightforward disclosures, and coordinated enforcement by the Information Regulator and the National Consumer Commission. The example of South Africa shows how continuous enforcement of clear consumer rights strengthens the integrity of online markets and encourages ethical business practices.

When taken as a whole, these jurisdictions demonstrate that proactive consumer education, competent regulators, and clear legislation are necessary for effective e-commerce consumer protection. Tanzania can reduce consumer vulnerability and increase trust in online transactions by implementing similar tactics, such as harmonising overlapping legislation, bolstering institutional capacity, and raising public understanding of digital rights.

CONCLUSION

The evaluation of Tanzania's e-commerce legal framework reveals a persistent and structural paradox which is, despite the country's adoption of contemporary laws intended to control digital transactions and safeguard consumers, such as the Electronic Transactions Act, Cap 442 R.E. 2023, the Fair Competition Act No. 13 of 2024, the Cybercrimes Act No. 14 of 2015, and the Personal Data Protection Act No. 11 of 2022, their actual capacity to protect online consumers. Regulatory reports, court rulings, and internet user experiences all

consistently show this disconnect between law and practice. Although cases concerning fraud, impersonation, unauthorised data usage, deceptive digital ads, and unsecure financial technology continue to increase, courts acknowledge electronic records, digital contracts, and online conversations as legitimate and enforceable under the Electronic Transactions Act (ETA), Cap 442 R.E. 2023. These patterns show that the legal safeguards included in the statutes do not provide consumers with significant security in their regular online transactions.

At the core of this conundrum are still institutional flaws. The Fair Competition Commission (FCC), the Tanzania Communications Regulatory Authority (TCRA), Bank of Tanzania (BOT), and law enforcement agencies have limited investigative capabilities, little knowledge of digital forensics, and poor interagency cooperation. Because of this, enforcement frequently focusses on specific criminals rather than structural flaws in online marketplaces and digital service providers. Low consumer awareness is equally significant; many Tanzanians are still unaware of their rights under the Personal Data Protection Act No. 11 of 2022, the Fair Competition Act, or the Electronic Transactions Act (ETA), Cap 442 R.E. 2023, which results in underreporting of infractions and a restricted pursuit of remedies. The lack of consistent digital-commerce standards among agencies, overlapping authorities, and disparate regulatory obligations all exacerbate this.

Comparative analysis from benchmark nations like South Africa, Kenya, and the EU emphasises Tanzania's difficulties even more. These nations show that active platform responsibility, strong oversight organisations, uniform regulations, and ongoing digital literacy programs are necessary for effective consumer protection in e-commerce, in addition to legal adoption. These practical elements are absent from Tanzania's existing structure, notwithstanding its legal soundness. As a result, its e-commerce laws' protective capacity is still mainly theoretical, which perpetuates the paradox that having complete legal tools does not ensure meaningful consumer protection.

Overall, the article finds that there is still insufficient regulation of Tanzania's online economy. The nation's sophisticated legal system will remain a symbolic rather than practical protection for online shoppers unless institutional capacity is increased, regulation overlaps are clarified, enforcement is strengthened, and public literacy is raised.

RECOMMENDATIONS

The article puts forward the following recommendations:

i. Create a specialist Digital Consumer Protection Authority to regulate online marketplaces, coordinate enforcement, and combine the various regulatory requirements that are now in existence.

ii. Increase institutional capacity by funding digital forensics equipment, educating employees, and fostering interagency collaboration between the FCC, TCRA, BOT, and law enforcement agencies.
iii. Establish strict platform-accountability requirements, mandating digital platforms and online merchants to provide correct information, safe payment methods, and open dispute resolution processes.
iv. Educate the public about online fraud dangers, e-commerce rights, and available redress methods by implementing national consumer awareness and digital literacy programs.
v. To improve legislative coherence and strengthen cross-border consumer protection, harmonise Tanzania's e-commerce laws with regional and global norms, especially the EU GDPR principles, Kenya's DPA, and South Africa's CPA.
vi. The Electronic Transactions Act (ETA), Cap 442 R.E. 2023 should be amended to include more explicit consumer-specific protections such mandated disclosures, cooling-off periods, and increased liability for digital misrepresentation.
vii. To ensure consistent implementation of the law, strengthen judicial guidance by creating practice guidelines on the management of electronic evidence, online contract disputes, and digital consumer claims.

FUTURE STUDIES

Future studies should examine the ramifications of regulatory consolidation and the effectiveness of enforcement mechanisms. Law enforcement and regulatory agencies should prioritise their capacity for digital forensics. We must examine platform liability for transactions involving third parties and the judicial interpretation of digital evidence. Studying consumer responses to fraud, data misuse, and dispute resolution in real-life scenarios is essential. This involves examining how AI-driven analytics can detect consumer harm and identify internet threats.

Academic emphasis should include internet literacy, consumer awareness, and access to grievance mechanisms. It is essential to examine the impact of AI-driven platforms and IoT-connected services on individuals' trust and their capacity to provide informed consent. A comparative review of alignment with international norms, particularly the EU GDPR and regulatory frameworks from Asia and Latin America, is recommended. A multidisciplinary study should assess the use of AI and IoT in compliance monitoring, smart contracts, and online dispute resolution, as well as their implications for consumer welfare, innovation, competitiveness, and regulatory effectiveness in Tanzania.

REFERENCES

Agibalova, T., Ivanova, M., & Petrov, A. (2020). *Digital consumers: Opportunities and risks in the online marketplace*. Journal of Digital Economy Studies, 5(2), 1–15.

Breakthrough Attorneys. (2022, February 10). *Banking and finance law update*: What should financial service providers know about protection of financial consumers in Tanzania? http://www.breakthroughattorneys.com

Bouke, M. A., Abdullah, A., Alshatebi, S. H., et al. (2023). *African Union Convention on Cyber Security and Personal Data Protection: Challenges and future directions*. Journal of African Cyber Law / Security, African Union Convention on Cyber Security and Personal Data Protection: Challenges and future directions.

European Union. (2011). *Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights. Official Journal of the European Union*.

European Union. (2022). *Digital Services Act (Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022). Official Journal of the European Union.*

George, J., & Simi, P. (2019). *Consumer rights and digital protection*: A global review. International Journal of Consumer Law, 7(1), 85–104.

Harvey, V., King, L., Wright, M., Chen, R., & Wood, C. (2022). *Consumer protection in global e-commerce transactions*. Journal of International Commercial Law & Technology, 3(1), 20–23

Hoercke, H. (2011). *Research methodology in law*. London: Oxford Academic Press.

Kaukab, R. S. (2025). *Consumer protection and e-commerce: Issues for developing country policy-makers.* International Institute for Sustainable Development.

Mambi, A. J. (2015). Cybercrime and Legal Framework in Tanzania: An Analysis of the Cybercrimes Act No. 14 of 2015. University of Dar es Salaam Law Journal, 38(1), 67–89.

Mambi, A. J. (2019). *The Legal Framework for Cybercrime Control and E-Commerce in Tanzania: Challenges and Prospects*. East African Journal of Law and Ethics, 5(1), 45–68.

Manteaw, S. (2020). *Electronic commerce and consumer protection in Ghana.* International Journal of Novel Research and Development

Masebu, G. (2021). *Consumer Protection in Tanzania's E-Commerce Framework*. Dar es Salaam University Law Journal, 14(2), 55–78.

Mwasomola, U. (2020). *Examining the consumer protection and comprehensiveness in e-commerce in Tanzania. Business and Economic Journal*, 11(5), 1–10. https://doi.org/10.35248/2151-6219.20.11.376

Mwenegoha, T. (2015). *The Development of Consumer Protection Laws in Tanzania for Electronic Consumer Contracts.* Doctoral thesis, Bond University.

Ndung'u, N. (2020). *Digital Literacy and Consumer Awareness in East Africa*. Nairobi: Strathmore University Press.

OECD. (2016). *Guidelines for consumer protection in the context of electronic commerce*. Organisation for Economic Co-operation and Development. https://doi.org/10.1787/9789264255258-en

Oreku, G. S. (2013). *A viewpoint of Tanzania e-commerce and implementation barriers*. Journal of Emerging Trends in Computing and Information Sciences, 4(9), 696–701.

Riefa, C., Coll, E., Gillies, L., Hunter, J., Simpson, R., Law, S., Scholten, M., Kaya, S., Goanta, C., & Aade, L. (2022). *Cross-border enforcement of consumer law: Looking to the future (Report to UNCTAD Working Group Sub-Working Group 3)*. University of Reading / UNCTAD.

Targański, B. (2020). The legal aspects of consumer protection in cross-border e-commerce. Digital Internationalization of Firms, 223-241 , 2025

The Electronic and Postal Communications Act, Cap. 306, Revised Edition 2022.

The Electronic and Postal Communications (Consumer Protection) Regulations, Government Notice No.427 of 2011.

The Electronic Transactions Act, Cap 442 Revised Edition 2023.

The Fair Competition Act No.13 of 2024 of the Laws of Tanzania.

The Fair Competition Commission Guidelines to Consumer Protection, Provisions in The Fair Competition Act, 2003.

UNCITRAL. (1996). *Model law on electronic commerce with guide to enactment.* United Nations Commission on International Trade Law.

Wang, H. (2019). E-*commerce regulation in China: Safeguards and challenges*. Journal of Asian Business Law, 14(3), 215–232.