

**REGULATION OF CONSUMER PROTECTION IN THE DIGITAL
ECONOMY IN TANZANIA**

DEODATUS P. SOKA

**A DISSERTATION SUBMITTED IN PARTIAL FULFILMENT OF THE
REQUIREMENT FOR THE AWARD OF MASTER OF LAWS (LL.M)**

**DEPARTMENT OF PRIVATE LAW
THE OPEN UNIVERSITY OF TANZANIA**

2024

CERTIFICATION

The Undersigned certify that he have read and hereby recommend for a Dissertation entitled, Regulation of Consumer Protection in the Digital Economy in Tanzania; in partial fulfilment for the Award of Masters Degree of the Open University of Tanzania.

.....

Dr. Abdallah Ally

(Supervisor)

Date.....

COPYRIGHT

This Dissertation is copyright material protected under the Copyright and Neighbouring Rights Act, No.7 of 1999 and other international and national enactments, in that behalf, on intellectual property . It may not be reproduced by anymeans, in full or in part except for short extracts in fair dealings, for research or private study, critical scholar review with acknowledgement, without the written permission of the Author Directorate of postgraduates' studies, on behalf of the author or Open University of Tanzania in that behalf.

DECLARATION

I, **Deodatus P. Soka**, do declare hereby that this Dissertation is my own original work and that it has not been presented and will not be presented to any other University for a similar or any other degree award.

.....

Signature

.....

Date

ACKNOWLEDGEMENTS

I appreciate my supervisor, Dr. Abdallah Ally for his wise guidance and timely responses which propounded towards accomplishment of this study. I also thank my work and school mates for being very cooperative with relevant inputs and important leads in the course of this study.

DEDICATION

Dedicated to my sons Praygod, Shawn and Parth for their perserverance throughout the years of accomplishing this dissertation .

LIST OF ABBREVIATIONS

CPA	Civil Procedure Act
EPOCA	Electronic and Postal Communication Act
Ibid	Ibidem - in the same source above
ICCPR	International Covenant on Civil and Political Rights
Idem	Already cited or used above
IT	Information Technology
OECD	Organization for Economic Co-operation and Development
PIA	Protection Impact Assessment
TCRA	Tanzania Communication Regulatory Authority
TTCL	Tanzania Telecommunication Company Limited
UDHR	Universal Declaration of Human Rights
UNESCO	United Nations Educational, Scientific and Cultural Organization
UN	United Nations
UNGCP	United Nations Guidelines on Consumer Protection

LIST OF INTERNATIONAL INSTRUMENTS

United Nations Guidelines on Consumer Protection (UNGCP)

World Trade Organization (WTO)

International Consumer Protection and Enforcement Network (ICPEN)

REGIONAL INSTRUMENTS

African Union Convention on Cyber Security and Personal Data Protection

East Africa Community Competition Act, 2006

LIST OF LEGISLATION

Principle Legislations

The Constitution of United Republic of Tanzania CAP 2 R.E. 2002

The Bank of Tanzania Act CAP 197 R.E. 2006

The Access to Information Act No. 6 of 2016

The Banking and Financial Institutions Act CAP 342 R.E. 2006

The Electronic and Postal Communications Act No. 03 of 2010

The Electronic Transactions Act No. 13 of 2015 G.N. No. 22 of 2015

The Finance Act No. 2 of 2014

The Finance Act No. 2 of 2016

The National Payment Systems Act No. 4 of 2015, G.N. No. 22 of 2015

Subsidiary Legislations

The Electronic and Postal Communications (Consumer Protection) Regulations, 2018

The Electronic and Postal Communications (Online Content) Regulations, 2020

The Banking and Financial Institutions (Capital Adequacy) Regulations G.N. No. 290/2014

LIST OF CASES

Stella Masha v. Tanzania Oxygen Limited (2003) TLR 64

Star Services Co. Ltd v. Railways Corporation (1989)1 HC

Felthouse v Bindley [1862] EWHC CP J35 Court of Common Pleas

Fisher v Bell [1961] 1 QB394

Pharmaceutical Society of Great Britain v Boots Cash Chemists 7 (1953)1 QB 401

Carlill v. Carbolic Smoke ball Company (1893)1 QB 256

Ford Motor Co. Ltd v AEF, 1 WLR 339, 1969

Jones v. Padavatton 3 [1969] 1 WLR 328 Court of Appeal

Entores v. Miles Far East (1955) 2 QB 327 (CA).

Pandit v.Sekawa 1964 (2) A.LR Comm.25

ABSTRACT

The dissertation investigates the regulation of consumer protection in the digital economy in Tanzania. It examines the conceptual and theoretical framework of e-

commerce in Tanzania, including the formation of contracts and the key challenges consumers face, such as security, privacy, jurisdiction, and dispute resolution. The study employs a doctrinal legal research approach, analyzing existing consumer protection laws, regulations, and international instruments. It includes comparative legal research to draw lessons from jurisdictions like Kenya and South Africa, as well as an evaluation of best practices from international frameworks such as the United Nations Guidelines on Consumer Protection. It analyzes the legal challenges facing the consumer protection framework in Tanzania and provides recommendations based on international best practices. The dissertation also explores the experiences of consumer protection regulation in other jurisdictions, such as Kenya and South Africa, to draw lessons for Tanzania. Additionally, it examines the legal and regulatory framework governing the digital economy in Tanzania, including relevant legislation and the role of regulatory authorities. The results of this study may provide valuable insights for educational leaders, policymakers, and researchers seeking to improve the gravity of e-commerce consumer protection. The study concludes with a summary of key findings and provides recommendations to strengthen the regulation of consumer protection in the digital economy in Tanzania, including the need for comprehensive legislation, enhanced consumer awareness, effective dispute resolution mechanisms, and improved coordination among regulatory bodies.

TABLE OF CONTENTS

CERTIFICATION ii

COPYRIGHT iii

DECLARATION	iv
ACKNOWLEDGEMENTS	v
DEDICATION	vi
LIST OF ABBREVIATIONS	vii
LIST OF INTERNATIONAL INSTRUMENTS	viii
REGIONAL INSTRUMENTS	viii
LIST OF LEGISLATION	viii
LIST OF CASES	ix
ABSTRACT	x
CHAPTER ONE	1
INTRODUCTION AND BACKGROUND TO THE PROBLEM	1
1.1 Introduction	1
1.2 Statement of the Problem	8
1.3 General Objectives	10
1.3.1 Specific Objectives.....	10
1.3.2 Research questions	10
1.4 Literature Review	11
1.5 Research Methodology	17
1.5.1 Doctrinal Legal Research.....	19
1.5.2 Comparative legal research	20
1.6 Data Analysis	21
1.7 Significance of the Study	22
1.8 The organization of the study.....	23
CHAPTER TWO	25

CONCEPTS, PRINCIPLES AND THEORIES RELATING TO CONSUMER

PROTECTION IN DIGITAL ECONOMY	25
2.1 Introduction	25
2.2 Digital Economy in relation to Tanzania	26
2.3 General Concept of E-commerce in Tanzania	27
2.4 Mobile Money	28
2.5 Categories of E-commerce	31
2.5.1 Business-to-business (B2B)	31
2.5.2 Business-to-consumer (B2C)	31
2.5.3 Consumer-to-consumer (C2C)	32
2.5.4 Consumer-to-business (C2B)	32
2.5.5 Business-to-administration (B2A)	32
2.5.6 Consumer-to-Administration (C2A)	33
2.6 Formation of Contracts in E-commerce Transactions	33
2.7 Problems E-commerce Consumer Face in Tanzania	40
2.7.1 Security and Privacy Concern	40
2.7.2 Jurisdiction & Appropriate Dispute Resolution	44
2.8 Theories	47
2.8.1 Information Asymmetry Theory	47
2.8.1.1 Implications for Consumer Protection	47
2.7.2 Behavioral Economics:	47
2.7.2.1 Implications for Consumer Protection	48
2.7.3 Contract Theory	48
2.7.3.1 Implications for Consumer Protection	48

2.7.4	Market Failure Theory	48
2.7.4.1	Implications for Consumer Protection	48
2.7.5	Rights-Based Approach	49
2.7.5.1	Implications for Consumer Protection	49
2.7.6	Fairness and Equity Theory	49
2.7.6.1	Implications for Consumer Protection	49
2.7.7	Product Liability and Safety	49
2.7.7.1	Implications for Consumer Protection	49
2.7.8	Consumer Empowerment.....	50
2.7.8.1	Implications for Consumer Protection	50
2.8	Conclusion	50
CHAPTER THREE		51
INTERNATIONAL AND REGIONAL INSTRUMENTS REGULATING		
CONSUMER PROTECTION IN THE DIGITAL ECONOMY		51
3.1	Introduction	51
3.2	International Instruments Regulating Consumer Protection.....	52
3.2.1	United Nations Guidelines on Consumer Protection (UNGCP).....	52
3.2.1.1	Basic Principles of the UNGCP	53
3.2.1.2	Implementation of the UNGCP.....	53
3.2.1.3	Challenges in Implementation.....	54
3.2.1.4	Benefits Achieved	55
3.2.2	World Trade Organisation (WTO).....	56
3.2.2.1	Basic Principles of the WTO Instrument	56
3.2.2.2	Implementation of the WTO Instrument.....	57

3.2.2.3	Challenges in Implementation.....	58
3.2.2.4	Benefits Achieved	58
3.2.3	International Consumer Protection and Enforcement Network (ICPEN)..	59
3.2.3	Shortcoming of ICPEN	62
3.2.4	African Union Convention on Cyber Security and Personal Data Protection	63
3.2.4.1	Shortcoming of the Malabo Convention	65
3.2.5	The East Africa Community Competition Act, 2006.....	66
3.2.5.1	Challenges of Implimenting the Act	69
3.3	Recommendations basing on International and Regional Instruments	70
3.4	Conclusion	70
CHAPTER FOUR.....		72
EXPERIENCE FROM OTHER JURISDICTION: LESSON FOR TANZANIA		72
4.1	Introduction	72
4.2	Kenya	72
4.2.1	Kenya Legal Framework.....	73
4.2.1.1	Communications (Electronic Transactions) Regulations, 2009.....	73
4.2.1.2	The Small Claims Court Act, Cap 10A (R.E. 2002).....	74
4.2.1.3	The Competition Act.....	75
4.2.1.4	The Consumer Protection Act.....	76
4.2.1.5	The Data Protection Act of 2019	76
4.3	South Africa	77
4.3.1	The Protection of Personal Information Act 2013 (POPIA).....	78

4.3.2	The Electronic Transactions and Communications Act 2002 (ETCA).....	79
4.3.3	The Consumer Protection Act 2008.....	80
4.4	Conclusion	81
CHAPTER FIVE.....		82
LEGAL FRAMEWORK GOVERNING DIGITAL ECONOMY IN		
TANZANIA		82
5.1	Introduction	82
5.2	Tanzania Legal Framework.....	82
5.2.1	The Electronic Transactions Act No.13 of 2015.....	83
5.2.2	The Cybercrimes Act, 2015	83
5.2.3	The Electronic and Postal Communications Act No.3 of 2010 (EPOCA) ...	84
5.2.4	The Electronic Money Regulations 2015.....	85
5.3	Strategy and Policies	86
5.3.1	Tanzania Digital Economy Strategic Framework 2024 - 2034.....	86
5.3.2	The National ICT Policy 2023	88
5.3.3	The National Records and Archives Management Policy, 2011	89
5.4	Legal Challenges facing Consumer Protection Framework in Tanzania....	89
5.5	Regulatory framework	92
5.5.1	Tanzania Computer Emergence Response Team TZ-CERT	93
5.5.2	Tanzania Data Protection Commission.....	94
5.5.3	Tanzania Communications Regulatory Authority	95
5.5.4	Fair Competition commission.....	96
5.4	Comperative Analysis Between Tanzania, South Africa and Kenya.....	97
5.7	Conclusion	99

CHAPTER SIX	100
SUMMARY OF FINDINGS, CONCLUSION AND RECOMMENDATIONS	
.....	100
6.1 Summary of findings.....	100
6.2 The study.....	101
6.3 Conclusion	101
6.4 Recommendation.....	102
BIBLIOGRAPHY	104

CHAPTER ONE

INTRODUCTION AND BACKGROUND TO THE PROBLEM

1.0 Introduction

The digital economy refers to an economic system that is based on digital computing technologies.¹ It encompasses all economic activities that rely on the internet, digital platforms, and other digital technologies to operate. This includes digital economy, online services, digital content, digital payments, and other forms of economic activity that are facilitated by the internet. It is not limited to just technology and internet companies.² Traditional sectors like agriculture, manufacturing, services, and retail can be part of the digital economy too, if they use digital technology to improve their operations, products, or services. The digital economy is characterized by its high velocity, broad impact, and potential for exponential growth. It is transforming industries, changing business models, influencing consumer behavior, and reshaping how work is conducted.³

Digital Economy is comprised of related components in comparison to other form of doing business particularly in exchanging of value for money with the requisite products, this mode of transaction becomes complete when the seller and buyer (consumer) accomplishes their agreed terms towards their transaction. Due to the

¹ Carl; Dahlman, Sam; Mealy, and Wermelinger, M (2016). "Harnessing the Digital Economy for Developing Countries," *OECD Development Centre Working Papers*, no. 334: 1–77. Retrieved from <https://www.oecd-ilibrary.org/docserver/4adffb24-en.pdf?expires=1674044903&id=id&acname=guest&checksum=1249F8F04498C0B269E3044B0436DBD8>.

² Atikah, I. (2020). "Consumer Protection and Fintech Companies in Indonesia: Innovations and Challenges of the Financial Services Authority," *Jurnal Hukum Dan Peradilan* 9, no. 1: 132, <https://doi.org/10.25216/jhp.9.1.2020.132-153>.

³ Mwakatumbula, H. (March 2017). "Consumer Protection in the Telecommunication Markets in the Post Liberalization Era-the Case of Tanzania. PhD Thesis, Graduate School of Asia-Pacific Studies

advancement of science and technology there are various means where a seller and buyer (consumer) meets each other like through online platforms, Radio and Television broadcast, online applications and adds. This mode of operation in the digital economy may put the consumer in a vulnerable environment where they might either lose their resources or threatens privacy of their personal information as the result of the existing gape on technological awareness for those who engage themselves in digital economy modes of doing business.⁴

In the realm of the digital economy, a consumer is any individual who avails themselves of digital services and platforms to purchase goods, obtain services, or interact within the virtual domain, spanning activities like online shopping, utilizing e-services, engaging in electronic communications, and participating in digital platforms for entertainment, education, or other purposes.⁵ The necessity to protect consumers emanates from the potential risks and threats pervasive in the digital space, including but not limited to, fraud, data breaches, privacy invasion, and cyber-attacks.⁶ Protecting consumers is not merely safeguarding them from financial losses but also ensuring the security of their personal information, safeguarding their digital identities, and fostering trust in digital platforms. This involves legal frameworks that not only counteract deceptive practices, safeguard privacy, and ensure data security but also enhance user confidence in electronic transactions, contributing

⁴ ITU webinars(November 2021).Consumer Protection in the Digital age, Data Privacy and Protection.

⁵ Digital economy report pacific report. Digital platforms,e-commerce and value creation and capture (2022) retrived from https://unctad.org/system/files/official-document/dtlecdc2022d4_ch3_en.pdf/

⁶ Maryland review.cyber security and data breach harms(2023). Retrieved from <https://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?article=3969&context=mlr>

fundamentally to the stable and sustainable growth of the digital economy. Ultimately, protected consumers are empowered to navigate, interact with, and contribute to the digital economy confidently, thereby nurturing its development and proliferation.

Thus, evolution of internet users can be traced from 1960's where there Consumer protection in the ICT sector has undergone significant transformation due to technological changes the reports shows that the use of mobile phones has also forstered mobile money transfer like through M-PESA, Tigo-PESA, Airtel Money etc what to note is that the increase on the use mobile phones has not only contributed on the development of mobile money transfer but it accompanied with the advent og the digital era particularly in the use of internet.⁷ The high increase on the rates of internet users in Tanzania is the proof of the contribution made by digital economy in enhancing the country economy, the report shows that the country's internet penetration rate has increased from 10.6% in 2015 to 48.5% in 2022, while mobile phone penetration has reached 90.1%.⁸ However this increase on internet users has negative impact in terms of peoples privacy and overall security due to the fact that most of Tanzanians are not aware on the ongoing development in science

⁷ Mashenene R. The Dynamics of Mobile Phone Technologies and the Performance of Micro and Small Enterprises in Tanzania (July 2015). Ritrieved on February 2024 from <https://www.researchgate.net/publication/281066150> The Dynamics of Mobile Phone Technologies and the Performance of Micro and Small Enterprises in Tanzania

⁸ TCRA Report: Internet and Social Media Usage, what should we Expect Rising Cyber Threats? (2023). Ritrieved on 20 March, 2024 from <https://www.digest.tz/tcras-2023-report-internet-and-social-media-usage>

and technology as the results most of them are vulnerable towards their basic rights like right to privacy as part of the negative effects of technological advancements.

Since, laws and practices are vital part of digital economy particularly in consumer protection as it is centered on trust, consumers might fall on traps of un-trustable and deceptive sellers who don't allow thorough opportunity for the consumer to evaluate, determine and even compare specifications of their needs with what is offered by the online seller.⁹ Furthermore setting of inaccurate information concerning a specific good ordered by the buyer/consumer can also be determined as among of the problems facing consumers in the current Digital economy

In Tanzania, despite the fact that Digital economy has the potential to accelerate business development through increased efficiency and reduced costs in business operations. It provides new business opportunities by facilitating access to foreign markets. It also allows businesses to participate in new activities, such as data and records processing, customer service and call centers, and software application development. In fact, numerous governments have announced that fostering digital economy is a major public policy objective to achieve economic growth.¹⁰

⁹ Mtaita,G.,Mayala,N and Amos,A. (2021) “Assessment of the Practice of Digital Disbursement Financial System in Managing Student’s Loans among Higher Learning Institutions in Northern Zone Tanzania,” Asian Journal of Humanities and Social Studies 9, no. 4: 170–80, <https://doi.org/10.24203/ajhss.v9i4.6746>.

¹⁰ Mutagahywa, B. (2000). Connectivity and E-commerce, Economic and Social Research Foundation (ESRF), UDSM.

As a result, in the recent years, digital technology has brought about significant changes to various sectors of the economy in Tanzania. For example, one can now perform banking transactions via a mobile device, such as, sending money, paying bills and paying taxes through an electronic money platform. Furthermore, government services are also conducted digitally, this have been facilitated after the establishment of Electronic Government Authority (e-Ga) by the e-Government Act of 2019 whereby under Section 4 among of the core functions of the authority is to promote e-Government research,development and innovation in public institutions and facilitation of public access to e-Government services.

However without subjudice to the positive outcomes of the digital economy for the development of the country as illustrated above, consumers in Tanzania are still vulnerable on the impacts of the said technology, thus misuse of consumers data for their personal benefits this has somehow now have been legislatively recognized through the enactment of the e-Government Act thus is regard to the paragraph above the authority which is also tasked with the administration, management and operations of e-Government services and provides for the management of electronic data and other incidental matters.¹¹

The Electronic Transactions Act, Number 13 of 2015, Chapter 442 of the laws of Tanzania, as amended from time to time (hereinafter referred to as the Electronic Transactions Act”) is the primary legislation governing electronic transactions in

¹¹ Quinta,Q (2013),’ Electronic Journal of e-Government, Initiatives in Sub-Saharan Africa. A Literature Review. Volume 11, Issue 2

Tanzania. Generally, electronic evidence and electronic signatures emanate from electronic transaction/s which have a component which is done or documented electronically.¹² However, In Tanzania, such transactions (except for the admissibility of electronic evidence in Court) were not legally recognized until the Electronic Transactions Act came into force on the 1st September, 2015. Despite of the Laws enacted to govern Electronic Transactions thus Electronic Transactions Act, consumers in Tanzania are still vulnerable and rampantly affected by ill move by those who tend to hide or register wrong personal identification while making transactions or while offering electronic transaction services.

On the other hand the Central Bank of Tanzania assuming its functions has also issued the Consumer Protection Regulations known as the Bank of Tanzania (Financial Consumer Protection) Regulations¹³ for the same purposes of protecting consumers. The Regulations set the mandatory requirements for all banking and Financial Institutions operating in Tanzania to have in place a Consumer Protection governance mechanism. The Regulations expressly define Financial Consumer protection to include laws, institutions, practices and policies to safeguard consumer rights, enable consumers to make informed financial decisions and ensure fairness in the provision of products and services by financial service providers regulated by the Central Bank. However, non-adherence of the procedures set by the Central Bank and lack of awareness of the consumers on the surrounding threats caused by the

¹² Mollel E. (2016) "The Legal Basis of Electronic Banking". LL.M Dissertation University of Dar es salaam.

¹³ 2019 GN No. 884 of 2019

advancement of science and technology has resulted to loss on some of the banking services users like voluntary or involuntary sharing of Personal Identification Number (PIN)¹⁴

Moreover, the ethos of the Arusha Declaration implied a government responsibility to safeguard the welfare and interests of its citizens, which in a broader interpretation, can be seen as encapsulating consumer protection rights within a framework that prioritizes communal well-being and safeguards against exploitation and inequity. After the Arusha declaration in Tanzania, consumer was accorded protection through government policies and by the legal, judicial and administrative arms of the state which lead to enactment of consumer protection laws in different sectors. The eventual development of consumer protection in Tanzania would however need to consider the advancements in technology and the evolving nature of consumer interactions in the digital age, extending beyond the socio-economic parameters set forth in the Arusha Declaration.

The dynamisms nature of culture and the ways people keep on advancing, it is observed that technology transform the speed of information rapidly to an extent consumer's safety can easily be invaded, leading to absence of confidentiality and lack of confidence among people in the society . Despite all these advancements by the Government and its agency to try to protect consumers, Tanzania legal sectors and judiciary has not yet enacted specific laws to regulate for example, interception

¹⁴ The Tanzania Regulatory Authority Act, 2003

of communication, lay down procedures for the interception, offences which will call for prosecution and enhance responsible Government Agency in protection of consumers.

1.1 Statement of the Problem

The swift evolution of the Internet, the expansive domain of e-commerce, and the continuous influx of technological innovations have introduced a new era of challenges for policymakers focused on consumer protection. In the Tanzanian context, the current Consumer Protection framework, primarily rooted in the Constitution of the United Republic of Tanzania, 1977, and reinforced by the Fair Competition Act, 2003, faces limitations in effectively addressing the unique aspects of consumer protection in the digital economy. Notably, the Tanzania National Electronic Banking Guidelines of 2007 lack legal enforceability, and even the recently enacted laws, the Cybercrimes Act, 2015, and the Electronic Transaction Act, 2015, do not thoroughly tackle issues specific to the digital economy. Similarly, the National Payment System, 2015, has failed to address key issues like e-cheque and customer protection.

Furthermore, the absence of a legally supported identification portal for valid sellers has led to significant resource losses for consumers. Additionally, technological advancements have facilitated the use of personal consumer information for personal gain, such as enticing consumers to purchase items they never intended to buy.¹⁵

¹⁵ Rangaswamy, E., Nawaz N., & Changzhuang Z., (15 March 2022). The impact of digital technology on changing consumer behaviours with special reference to the home furnishing sector in

Although constitutional and legislative provisions establish a foundation for consumer rights, the surge in online transactions, digital services, and technological advancements necessitates a more nuanced and adaptive approach. The existing laws, conceived in a pre-digital era, may not fully cover the intricacies and novel challenges brought about by the digital economy such as the lack of redress or recovery procedure in case the consumer has lost his resources after being involved in a business with un-trusted online seller.

On the other hand the Laws failed to determine treatment of conflicts originated from digital economy kind of business from different jurisdictional barriers as the matter of fact two parties who have been involved into a business transaction are mostly located in two different jurisdiction. Other Issues are like data privacy, online fraud, digital product safety, and the dynamics of electronic transactions present unprecedented challenges that also demand a reassessment of the existing legal framework. Gaps in consumer protection laws may expose consumers to exploitation, fraud, and other risks inherent in the digital marketplace. Consequently, there is an urgent need for policymakers to not only stay abreast of rapid technological changes but also proactively formulate and implement regulations specifically tailored to safeguard the interests of consumers in the digital age.

This problem statement emphasizes the pressing need for a comprehensive review and enhancement of the consumer protection framework in Tanzania to ensure its

relevance, efficacy, and responsiveness to the evolving landscape of the digital economy.

1.2 General Objectives

The primary aim of this dissertation is to assess the existing legal frameworks governing consumer protection within the digital economy in Tanzania. Specific Objective being to evaluate the current consumer protection laws in Tanzania and identify gaps that hinder effective protection in the digital marketplace.

1.2.1 Specific Objectives

- i. To identify legal gaps in the existing laws regulating consumer Protection in Tanzania's digital economy
- ii. To learn the experience of other jurisdictions with regards to Digital Economy and consumer protection
- iii. To gain experience in international legal instruments and best practice
- iv. To suggest a regulatory framework that promotes innovation and enhances consumer protection

1.2.2 Research questions

- i. What are the existing legal gaps in the laws regulating consumer protection in Tanzania's digital economy ?
- ii. What experience can be learn't from other jurisdictions regarding digital economy and consumer protection?

- iii. What are the international legal instruments and best practices that can provide valuable insights and experience in the field?
- iv. What regulatory framework can be proposed to effectively promote innovation while simultaneously enhancing consumer protection?

1.3 Literature Review

The rapid growth of the internet and e-commerce has revolutionized the way businesses operate and people engage in transactions. This part aims to explore the difficulties associated with safeguarding online customers and highlight the key factors and trends identified in the existing literature. One of the primary difficulties in protecting online customers is the ever-evolving landscape of cybersecurity threats. Malicious actors employ various techniques such as phishing,¹⁶ hacking, malware, and identity theft to exploit vulnerabilities in online systems, compromising the security and privacy of customers.

The lack of awareness and education among online customers is another significant challenge. Many customers are unaware of the potential risks associated with online transactions,¹⁷ making them more susceptible to fraudulent activities. Educating customers about best practices, such as using strong passwords and employing two-factor authentication, can help mitigate these risks.

¹⁶ A technique for attempting to acquire sensitive data such as Bank Account numbers, through a fraudulent solicitation in email or in a website, in which a perpetrator masquerade as a legitimate business or reputable person

¹⁷ Financial Consumer Protection in Tanzania (Institutional, Legal and Regulatory Framework) Presentation at the BOT Academy (22-23 November 2022)

Data breaches pose a severe threat to the protection of online customers. When organizations fail to secure customer data adequately, it can lead to identity theft, financial loss, and reputational damage. Customers are increasingly concerned about their privacy and the misuse of their personal information, creating a need for stronger data protection regulations. The legal and regulatory framework surrounding online customer protection is complex and often struggles to keep pace with technological advancements. Jurisdictional issues, inconsistent international laws, and difficulties in enforcement create challenges in holding perpetrators accountable and providing timely remedies to affected customers.

Another ongoing challenge is the Balancing of security measures with user experience and convenience. Implementing stringent security protocols can sometimes lead to cumbersome authentication processes or lengthy checkout procedures, potentially hampering the overall customer experience. Striking the right balance between security and convenience is essential to encourage customer adoption and retention. The global nature of online transactions adds another layer of complexity to customer protection efforts. Different countries have varying levels of cybersecurity infrastructure and legal frameworks, making it challenging to establish consistent standards and ensure uniform protection for customers worldwide.

According to Mambi, A.J (2010),¹⁸ in his book “ICT Law Book” is mostly relevant to this research as he stated clearly that the rapid growth of digital economy over the

¹⁸ Mambi, A. (2010). ICT Law Book; A Source Book for Information & Communication Technologies and Cyber Law, Mkuki na Nyota, Tanzania.

world has brought challenges and effects Tanzania's commercial offline laws and other related laws and the society at large given the nature of paper-based transactions. While Mambi's book offers a detailed analysis of the legal and regulatory framework governing Tanzania's digital market, it primarily focuses on the broader ICT sector, including telecommunications and electronic communications. The book did not delve deep into the specific consumer protection issues and challenges that are uniquely associated with the e-commerce domain, such as online payment systems, product quality and safety, and cross-border transactions. Therefore left a gap on the specific legal mechanisms and remedies available to consumers in the event of disputes or grievances related to e-commerce transactions. Nonetheless this work is relevant to this study in the aspect of legal and regulatory framework for the broader ICT sector.

Moreover Turban, E, King, D and Lee, J (2008)¹⁹ in the book titled "Electronic Commerce" briefly shows the reasons why the specific laws should be enacted to regulate the electronic contract. The laws must accommodate the rule and regulation of conducting distance selling contracts as the nature of distance selling contracts has got peculiar features contrast to traditional contract. However, while the book provides a comprehensive overview of consumer protection in the digital economy, it does not fully address some of the more specific and emerging legal gaps. For instance, the book does not extensively cover the legal implications of new

¹⁹ Turban E, King D, & Lee K.(2008). Electronic Commerce. A Managerial and Social Networking Perspectives, Person Education, U.S.

technologies, such as blockchain, cryptocurrency, and smart contracts, and how these innovations may impact consumer protection in the digital market. Nonetheless its relevancy to this study lies on the focus of protection of consumers on the fast growing technology sector which is the thrust of this study.

Reed, C, (2004),²⁰ in his book “Internet and Law, argued about the laws in most countries were developed over a long time during which the physical actors and physical media were the only, at least the primary, mechanisms by which transaction with legal consequences could be affected. Reed also emphasized the need for effective privacy laws and regulations to safeguard consumers' personal information and data in the context of online transactions.

Reed’s book focus is primarily on the broader context of internet law, without a specific emphasis on the e-commerce or digital market sector. While the legal principles and frameworks discussed in the book may be applicable to the digital market, the book does not provide a comprehensive analysis of the unique consumer protection challenges and corresponding legal solutions specific to the e-Commerce domain. Nevertheless its relevance to this study is based on the challenges of contracts in digital transactions and consumer protection in cross border market which is part of this study

²⁰ Reed, C. (2004). *Internet Law; Text and Materials* (2nd) Cambridge University Press, U.S.,.

Mollel (2016),²¹ exhausted a lot of electronic banking laws in Tanzania as to what laws regulate the banking system and particularly as to what laws govern electronic banking. Author established that money is being saved by not employing the bank tellers because now most things are automated and can be done in a gadget like mobile phones and computers through internet and applications.

However, Mollel's dissertation did not delve deeply into the broader e-Commerce consumer protection framework beyond the specific context of electronic banking. While electronic banking is a crucial aspect of the digital market, the dissertation does not extensively cover the legal and regulatory aspects of consumer protection in other e-commerce domains, such as online retail, digital services, or peer-to-peer transactions. Its relevancy to this study however lies on the focus of regulations that address issues such as data privacy, security, and liability allocation in electronic banking transactions.

Peitz and Waldfogel (2012),²² in their work titled the Oxford Handbook of the Digital Economy discusses how digital technologies are reshaping industries, altering consumer behavior, and influencing market structures. The authors addresses concerns related to data privacy, highlighting the importance of protecting consumer information in an increasingly data-driven economy. The book further provides insights into various regulatory approaches to managing the digital economy,

²¹ Mollel E. (2016). "The Legal Basis of Electronic Banking" LL.M Dissertation University of Dar es salaam,

²² Peitz, Martin, and Joel Waldfogel (eds), (2012). *The Oxford Handbook of the Digital Economy*, Oxford Handbooks; online edn, Oxford Academic, 21 Nov. 2012), <https://doi.org/10.1093/oxfordhb/9780195397840.001.0001>, accessed 24 Oct. 2024.

emphasizing the need for adaptive regulations that can keep pace with technological advancements.

Nonetheless while the handbook discusses various regulatory approaches, there is a lack of focus on how these frameworks can be specifically tailored to suit the legal and cultural environment of countries like Tanzania. Same goes for digital transformation, but does not deeply explore how these changes specifically affect consumer rights and protections in developing countries like Tanzania. Its relevancy to this study however is that, it serves as a critical resource for the dissertation, offering theoretical insights, regulatory comparisons, and empirical analyses that are essential for understanding and improving consumer protection in Tanzania's digital economy.

CIPESA (2015),²³ the Collaboration on International ICT Policy in East and Southern Africa highlights that governments have enacted various laws to facilitate the implementation of digital economy, however there are other laws which slow down and pose challenge on the implementation of e-government initiatives. Some of these laws were enacted over forty years ago and negatively impact meaningful citizen participation, the free flow of information, access to information and freedom of expression.

For consumers to contribute to the national economy in the industrial revolution era,

²³CIPESA, (October 2015) *ICT in Governance in Tanzania – Policies and Practice*, CIPESA ICT Research Series No. 07/15.

they need to be confident in the whole business process and the data flow. In this regard, data protection, privacy, and confidentiality are vital. This part reviews studies conducted in different parts of the world on issues related to confidentiality, data protection and the privacy of consumers. In the context of SNS, the requirement to secure "confidentiality of security of processing" also assumes a new dimension. In order to comply with this criterion, the controller must ensure that the personal data being processed is only revealed to those who "need to know." There are no limitations on who may view the information when the user's profile is set to public. However, even when the profile is set to private, most SNS still do not give users much discretion over which aspects of their profile should be available to which "friends" (Campbell, 2021). Protecting data privacy is still vital to consumers during the pandemic, according to the Cisco Consumer Privacy Survey report titled "Protecting Data Privacy to Maintain Digital Trust.

1.5 Research Methodology

The term 'research methodology', refers to a systematically way of solving' the research problem. It is a 'science of studying how research is done scientifically'. It involves a study of various steps and methods that a researcher needs generally to adopt in his investigation of a research problem along with the logic behind them. It is not only a study of methods but also of explanation and justification for using certain research methods and of the methods themselves. It includes in it the philosophy and practice of the whole research process. In other words, research methodology is a set of rules of procedures about the way of conducting research. It

includes in it not just a compilation of various research methods but also the rules for their application and validity.²⁴

Legal research specifically is ‘a systematic finding’ or ‘ascertaining’ law’ on the identified topic or in the given area as well as ‘an inquiry’ into ‘law’ with a view to making advancement in the science of law.²⁵ It is the process of identifying and retrieving information necessary to support legal decision-making. It includes in it each step of a course of action that begins with an analysis of the facts of a problem and concludes with the application and communication of the results of the investigation.²⁶

Legal research may be carried out by utilising one or more of number of different techniques or methodologies. These different methodologies include, inter alia, doctrinal research, comparative law methods, socio-legal methods and philosophical legal methods.²⁷ In this research, two methods, namely doctrinal research and comparative legal methods have been applied in the analysis of law. Besides, the comparative legal research has been applied to study legislative texts, jurisprudence and legal doctrines of foreign laws relating to regulation of mobile money services.

²⁴ Vibhute, K & Aynale, F (2009)., Legal research methods: Teaching material, pp.26

²⁵ Ibid pp.29

²⁶ Ibid pp.30

²⁷ Singhal, A.K & Malik, I., Doctrinal and socio-legal methods of research: merits and demerits, Educational Research Journal Vol. 2(7), pp. 252-256, July 2012 Available online at <http://www.resjourn> accessed 20th may 2014.

1.5.1 Doctrinal Legal Research

Doctrinal research is the most common methodology employed by those undertaking research in law. It entails the use of primary (statutes and case law) and secondary sources of law (reports, journal articles, text books and other forms of publication). Doctrinal research asks what the law is on a particular issue or context. It is concerned with analysis of the legal doctrine and how it has been developed and applied. This type of research is also known as pure theoretical research or black letter research. Under doctrinal methodology a researcher's main goal has been the analysis of statutes, cases, reports, publications and model laws as they relate to the subject matter under scrutiny.²⁸ This methodology entailed the use of various legal methods such as rules of statutory legal interpretations and legal reasoning both inductive and deductive in order to critically analyse the materials collected against the backdrop of the research questions.

This methodology has been very useful in the present study due to its potential in contributing to the development, continuity, consistency and certainty of law. Employment of this methodology has enabled this study, to analyse the existing law relating to e-commerce consumer protection, and to consider how the law ought to be in order to address the emergent challenges and risks whilst also it promotes innovation and technological advancement.

²⁸ Singhal, A.K & Malik, I. "Doctrinal and socio-legal methods of research" op.cit

1.5.2 Comparative legal research

This study has set forward comparative legal research in order to study legislative advancement, jurisprudence and legal doctrines of foreign laws for the sake of stimulating awareness of the legal framework and to gain insights and lessons that could be considered in addressing the challenges and to provide an insight concerning challenges of consumer protection in digital economy and the way such challenges can be mitigated in the country.

Since its commencement in the 20th Century, comparative law has played significant role in the science of legal interpretation in national courts, legal reforms as well as unification and harmonization of laws.²⁹ The essence of comparative law is the act of comparing the law of one country to that of another. Most frequently, the basis for comparison is a foreign law juxtaposed against the measure of one's own law. But, of course, the comparison can be broader: more than two laws, more than law, more than written words. It facilitates better understanding of the functions of the rules and principles of laws and involves the exploration of detailed knowledge of law of other countries to understand them, to preserve them, or to trace their evolution. Accordingly, comparative legal research is beneficial in a legal development process where modification, amendment, and changes to the law are required.³⁰

²⁹ Makulilo,A,B., Protection of Personal Data in sub-Saharan Africa, PhD Thesis, Bremen University,2012 pp.88

³⁰ Eberle, E.J., The method and role of comparative law, Washington University Global Studies Law Review, Volume 8 number 3, 2009

The most common comparative legal scholarship is cross jurisdictions comparison of laws of different legal systems. It is typical for researchers who undertake this research to examine the law as it is while at the same time provide ideas and views for future legal development.³¹ In this context, the researcher employed this method in examining the development of digital market consumer protection in foreign jurisdiction (South Africa and Kenya) which has the most strong consumer protection landscape in Africa.

The researcher has passed through, International and Regional Instruments on Consumer Protection, local laws, Strategies and Policies and Regulatory bodies in order to get best insights into best practices of digital economy consumer protection, best practices that can be used as a benchmark for institutional maturity and good governance when evaluating country-specific financial practices.³²

1.6 Data Analysis

Collected data regarding the study will be analyzed through different legal techniques and methods. Therefore, the study will employ inductive, deductive, and analogy techniques of legal reasoning and interpretation. In this regard, inductive and deductive methods will be used to analyze different data collected from general to specific and vice versa, and the analogy method of data analysis will be used to

³¹ Ibid

³² USAID. (2012), Standards and Practices Report for Electronic and Mobile Payments, , pp.18

compare the law and best practice as applied in selected jurisdictions in comparison with the legal framework applicable in Tanzania.

1.7 Significance of the Study

The study on consumer protection in Tanzania holds paramount importance for various stakeholders, especially academicians. The evolving regime that governs consumer protection in the nation has been riddled with complexities and challenges, necessitating an in-depth analysis and understanding. For the informed academician, this study isn't just about gaining knowledge but also about understanding the intricate balance that needs to be struck when it comes to protecting consumers. The dynamics of consumer protection aren't just legal; they are intertwined with socio-economic realities, cultural nuances, and the ever-evolving marketplace. As such, it's vital for scholars and experts to be equipped with a comprehensive understanding of the landscape. This will not only aid in academic pursuits but will also provide a roadmap for policy recommendations and potential legislative reforms.

Moreover, a thorough examination of Tanzania's consumer protection framework will unveil the existing gaps within the current laws. Identifying these gaps is the first step towards addressing them. Once we are aware of the lacunae, efforts can be channeled towards developing robust mechanisms that cater to the needs of the modern Tanzanian consumer, ensuring that their rights are safeguarded against malpractices and ensuring that businesses operate within a framework of fairness and transparency. In addition, by understanding the shortcomings and strengths of the existing system, academicians can play a crucial role in influencing policy changes.

They can provide insights based on empirical data, case studies, and comparative analysis, which can guide legislators in drafting laws that are both progressive and in tune with the demands of the contemporary market.

1.8 The organization of the study

The study will be organized into five chapters and shall cover the following;

Chapters One: The first chapter will be the general introduction, which is the existing chapter bearing among others, the background of the problem, the statement of the problem, objectives of the studies, literature review, the significance of the studies, methodologies, and chapter break up. The chapter is important for showing the roadmap on which the research will be conducted, and the theme therein.

Chapter Two; Concepts, Principles and theories Relating to Consumer Protection in digital economy.

Chapter three: International and Regional Instruments; In this chapter, the researcher will present among others, international instruments and regional instruments, that have taken into regard consumer protection and various problems facing consumers in the digital economy. This will include Laws, policy and even regulations which safe guard consumers rights like the right to privacy.

Chapter four: Experience from Other Jurisdictions; In this chapter, the research shall present experiences from other jurisdictions, on how the regime regulates consumers protection , their institutional framework, and practices. Such experience shall be taken from EAC.

Chapter five: Legal and Regulatory Framework governing consumer protection in Tanzania. The research will present both the legal framework and the Institutional

framework, whereby for the legal framework, the legal regime regulating consumer protection in Tanzania, by tracing historically and the current status.

Chapter Six: Summary of findings, Conclusion and Recommendations.

CHAPTER TWO

CONCEPTS, PRINCIPLES AND THEORIES RELATING TO CONSUMER PROTECTION IN DIGITAL ECONOMY

2.0 Introduction

The digital economy has emerged as a powerful force driving innovation, economic growth, and social transformation worldwide.³³ In the modern digital era, e-commerce has become an integral part of our daily lives. It has revolutionized the way businesses operate and transformed the way we buy and sell goods and services. But one have to wonder about the origins of e-commerce and how it all began? To understand the origin of e-commerce, we must first delve into the birth of the internet. The internet, initially developed as a military project called ARPANET in the late 1960s, was a network that allowed computers to communicate with each other. Over time, it evolved into a global network of interconnected computers, forming the foundation for e-commerce.³⁴ The real breakthrough for e-commerce came in the 1990's with the advent of the World Wide Web. In 1991, Tim Berners-Lee introduced the first web page, paving the way for the commercialization of the internet³⁵. This chapter is going to discuss the general concept, categories, formation and problems facing e-commerce in Tanzania.

³³ Mugume.R and Bulime.E (July 2022). "Post-COVID-19 Recovery for African Economies: Lessons for Digital Financial Inclusion from Kenya and Uganda."

³⁴ *ibid*

³⁵Home of science (2024) Retrieved from website on 23 February 2024 from <https://www.home.cern/science/computing/birth-web/short-history-web#:~:text=Tim%20Berners%2DLee%2C%20a%20British,and%20institues%20around%20the%20world> visited on 25th March 2024

2.1 Digital Economy in relation to Tanzania

The digital economy in Tanzania has experienced significant growth in recent years, bringing about a profound impact on consumer behavior and market dynamics. The key aspects ranges from; increased internet penetration, mobile money revolution, digital financial Services, data driven insights, online market growth, etc.

Recently, Tanzania has witnessed a rapid expansion of internet connectivity and mobile penetration. This has resulted in a large population gaining access to digital platform and services leading to a shift in consumer behavior.³⁶ The rise of digital market platforms in Tanzania has opened up new avenues for consumers to shop conviniently online eg. JUMIA, KIKUU etc.,. consumers can now access a wide range of products and services, compare prices, and make purchase comfortably from their homes. This has significantly impacted traditional retail markets and created new opportunity for business.³⁷ Another aspect impacted by the digital economy is Mobile money revolution. Tanzania has been at the forefront of the mobile money revolution with the introduction of services like M-Pesa,³⁸ etc., mobile money has transformed the way consumers make payments, conduct financial transactions, and access financial services,³⁹ especialy in rural areas where traditional banking

³⁶ Okeleke, K., (2019). Digital transformation in Tanzania – the role of mobile technology and impact on development goals. GSMA. Retrieved from <https://data.gsmaintelligence.com/api-web/v2/research-file-download?id=39256224&file=2736-180319-Tanzania.pdf>(Para 3) visited on 20th April 2024

³⁷ Ibid

³⁸ The EastAfrican. (2024). M-Pesa's revolutionary products stimulate socio-economic growth in Tanzania. Retrieved from <https://www.theeastafrican.co.ke/tea/sponsored/the-quiet-revolution-of-financial-inclusion-in-tanzania-4553260> visited on 17th April 2024

³⁹ Worldbank (2012). A bank in your pocket: The mobile money revolution in Tanzania. Rietrieved from <https://blogs.worldbank.org/en/african/a-bank-in-your-pocket-the-mobile-money-revolution-in-tanzania> (Para 5) on 17th April 2024

infrastructure is limited. Another aspect affected by the growth of digital market is the online Marketing and Advertisement. The digital economy has transformed marketing and advertising practices in Tanzania. Business are leveraging digital channels such as social medias etc to reach and engage with their target audience more effectively.⁴⁰ This in turn has led to a shift in advertising budget and strategy. Lastly but not least is Data-driven Insights, the digital economy generates vast amount of data, providing businesses with valuable insights into consumer behavior, preference and market trends.⁴¹ By harnessing data analytics, companies can make informed decisions, tailor their offerings, and enhance the overall consumer experience.⁴²

2.2 General Concept of E-commerce in Tanzania

E-commerce, short for electronic commerce, refers to the buying and selling of goods and services over the internet.⁴³ It involves conducting business transactions electronically, typically through online platforms or websites, henceforth E-commerce and digital are the two sides of the same coin as interdependent to each other. E-commerce enables individuals and businesses to engage in various commercial activities, such as online shopping, electronic payments, online auctions, and internet banking⁴⁴. Tanzania is one among the beneficiaries of the development of new technology. The trend of people doing business online has risen exponentially

⁴⁰ Ibid

⁴¹ <https://www.forbes.com/sites/forbesbusinessdevelopmentcouncil/2022/05/10/wy-data-driven-insights-are-critical-to-digital-transformation/?sh=3eb8784d78c2> (Para 3) visited on 17th April 2024

⁴² ibid

⁴³ The African Union Convention on Cyber Security and Personal Data Protection. Article 1

⁴⁴ International Trade Centre (2015). "International E-commerce in Africa. The way forward" 2015 at 4. Retrieved on 4th february 2024 from <https://intracen.or/file/internationalecommerceinafricalowrespdf>

in recent years. Studies show, up until 2021 in every 100 Tanzanian citizens 31.633 were active users of internet⁴⁵

In an e-commerce transaction, customers can browse and select products or services from online catalogs or websites, add them to a virtual shopping cart, and proceed to a secure online checkout process. Payment can be made using various methods, including credit cards, digital wallets, or online banking. After the payment is processed, the goods are typically shipped to the customer's specified address, or digital products are delivered electronically⁴⁶.

E-commerce has revolutionized the way businesses operate and how consumers shop. It offers several advantages, such as convenience, accessibility, a wide range of products and services, competitive pricing, and the ability to shop from anywhere at any time. E-commerce has also facilitated the growth of online marketplaces, where multiple vendors can sell their products on a single platform⁴⁷.

2.3 Mobile Money

In Tanzania, mobile money has played a significant role in financial inclusion and the development of the digital economy. Tanzania has seen a rapid adoption of mobile money services, with the country's mobile money penetration and according

⁴⁵ Economic Research Resources (1991). Retrieved on 25th March 2024 from <https://fred.stlouisfed.org/series/ITNETUSERP2TZA>

⁴⁶ Binding, J. & Purnhagen K. (2011). "Regulations on E-commerce Consumer Protection Rules in China and Europe Compared – Same Same but Different. Pg. 187

⁴⁷ *ibid*

the Fin Scope Tanzania 2023 Report sheds light on the uptake of formal financial services, with the adoption of mobile money increasing from 60% in 2017 to 72% in 2023.⁴⁸ This growth can be attributed to the widespread availability of mobile network coverage and the convenience offered by mobile money platforms. Also as well the mobile money market in Tanzania is dominated by two major players - M-Pesa (operated by Vodacom) and Tigo Pesa (operated by Tigo),⁴⁹ there are also other players like Airtel Money, Hallopesa etc. These service providers have built extensive agent networks across the country, making it easier for users to access and utilize mobile money services. Mobile money in Tanzania has also evolved beyond just person-to-person (P2P) transfers. It is now widely used for a variety of transactions, including bill payments, merchant payments, savings, and even loan disbursements and repayments.⁵⁰ This has helped to drive financial inclusion and provide access to financial services for the unbanked and underbanked population.

The Bank of Tanzania (BOT) has played a crucial role in developing a conducive regulatory environment for mobile money.⁵¹ The central bank has introduced

⁴⁸ Julia Seifert. Driving Mobile Money Usage in Tanzania through Expansion of Use Cases. Retrieved from <https://www.fsdt.or.tz/2024/03/18/driving-mobile-money-usage-in-tanzania/#:~:text=In%20recent%20years%2C%20Tanzania%20has%20witnessed%20a%20remarkable,from%2060%25%20in%202017%20to%2072%25%20in%202023> accessed on 31/05/2024

⁴⁹ Number of mobile money subscriptions in Tanzania from 2018 to 2023, by operator and quarter. Retrieved from <https://www.statista.com/statistics/1080805/tanzania-mobile-money-subscriptions-by-operator/#:~:text=The%20growing%20mobile%20money%20sector%20in%20Tanzania%20is,mobile%20money%20subscribers%20in%20Tanzania%20exceeded%2047.2%20million> accessed on 31/05/2024

⁵⁰ Evolution of Mobile Money Payment is Strengthening Financial Inclusion. Africa Press. Retrieved from <https://www.africa-press.net/tanzania/economy/evolution-of-mobile-money-payment-is-strengthening-financial-inclusion#:~:text=AfricaPress-Tanzania%3A%20MOBILE%20money%20services%20in%20Tanzania%20have%20evolved,to%20introduce%20interoperability%20between%20rival%20mobile%20money%20services>. Accessed on 31/05/2024.

⁵¹ Financial Markets. BOT. Retrieved from <https://www.bot.go.tz/FinancialMarket> accessed on 31/05/2024

guidelines and regulations to ensure the stability and security of the mobile money ecosystem, while also encouraging innovation and competition. Tanzania as a country has made progress in achieving interoperability between different mobile money platforms, allowing users to transfer funds seamlessly across networks.⁵² This has been a significant step in enhancing the overall user experience and fostering a more inclusive digital financial ecosystem.

Despite the successes, Tanzania's mobile money sector faces some challenges, such as the need for further consumer education, addressing the risks of cybercrime and fraud, and ensuring the affordability of mobile money services for low-income segments of the population.⁵³ Overall, the growth of mobile money in Tanzania has been a success story, contributing to financial inclusion, the development of the digital economy, and the empowerment of individuals and businesses across the country.⁵⁴

⁵² Evolution of Mobile Money Payment is Strengthening Financial Inclusion. Africa Press. Retrieved from <https://www.africa-press.net/tanzania/economy/evolution-of-mobile-money-payment-is-strengthening-financial-inclusion#:~:text=AfricaPress-Tanzania%3A%20MOBILE%20money%20services%20in%20Tanzania%20have%20evolved,to%20introduce%20interoperability%20between%20rival%20mobile%20money%20services>

⁵³ Julia Seifert. Driving Mobile Money Usage in Tanzania through Expansion of Use Cases. Retrieved from <https://www.fsdt.or.tz/2024/03/18/driving-mobile-money-usage-in-tanzania/#:~:text=In%20recent%20years%2C%20Tanzania%20has%20witnessed%20a%20remarkable,from%2060%25%20in%202017%20to%2072%25%20in%202023> accessed on 31/05/2024

⁵⁴ Financial Sector Deepening Trust (FSDT). (2021). The state of the Tanzanian mobile money market. Retrieved from <https://www.fsdtanzania.org/publications/the-state-of-the-tanzanian-mobile-money-market/> Accessed on 1st June 2024

2.4 Categories of E-commerce

Generally speaking, when most people think of e-commerce, they think of the purchase of goods or services by use of the internet. However, there is a more specific way to refer to the type of online transaction by the means of mentioning which e-commerce category the transfer falls under. E-commerce takes either the domestic (intra-border) route or cross-border (International) transactions. Invariably, six e-commerce models, i.e. Business-to-Consumer (B2C), Business-to-Business (B2B), Consumer-to-Business (C2B), Consumer-to-Consumer (C2C), Business-to-Administration (B2A) and Consumer-to-Administration (C2A) operate across countries⁵⁵.

2.4.1 Business-to-business (B2B)

B2B e-commerce refers to all electronic transactions of goods and sales that are conducted between two companies. This type of e-commerce typically explains the relationship between the producers of a product and the wholesalers who advertise the product for purchase to consumers. Sometimes this allows wholesalers to stay ahead of their competition.⁵⁶

2.4.2 Business-to-consumer (B2C)

Perhaps the most common form of e-commerce, B2C e-commerce deals with electronic business relationships between businesses and consumers. Many people

⁵⁵ Chawla N., & Kumar B., (July 2021). E- Commerce and Consumer Protection in India: The Emerging Trend Pg. 582

⁵⁶ Ibid., Pg. 583

enjoy this avenue of e-commerce because it allows them to shop around for the best prices, read customer reviews and often find different products that they wouldn't otherwise be exposed to in the retail world. This e-commerce category also enables businesses to develop a more personalized relationship with their customers⁵⁷.

2.4.3 Consumer-to-consumer (C2C)

This level of e-commerce encompasses all electronic transactions that take place between consumers. Generally, these transactions are provided by online platforms (such as PayPal), but often are conducted through the use of social media networks (Facebook marketplace, instagram *et al*) and websites.⁵⁸

2.4.4 Consumer-to-business (C2B)

Not the most traditional form of e-commerce, C2B e-commerce is when a consumer makes their services or products available for companies to purchase. An example of this would be a graphic designer customizing a company logo or a photographer taking photos for an e-commerce website⁵⁹.

2.4.5 Business-to-administration (B2A)

This e-commerce category refers to all transactions between companies and public administration. This is an area that involves many services, particularly in areas such as social security, employment and legal documents⁶⁰.

⁵⁷ Numinix; what are the different categories of e-commerce? (February 2023) Retrieved on February 2023 from <https://www.numinix.com/blog/what-are-the-different-categories-of-ecommerce/>

⁵⁸ Ibid

⁵⁹ Ibid

⁶⁰ Ibid

2.4.6 Consumer-to-Administration (C2A)

Another popular e-commerce category, C2A e-commerce encompasses all electronic transactions between individuals and public administration. Examples of this include taxes (filing tax returns) and health (scheduling an appointment using an online service⁶¹).

2.5 Formation of Contracts in E-commerce Transactions

The law of contract Act⁶² being the main law governing formation of contracts provide guidance for contractual arrangements.⁶³ The guidance are used to determine the validity or invalidity of a contract. It is easy to determine when a contract comes into existence in traditional commerce as the rules of common law and statutes stipulate what amounts to a valid contract⁶⁴. However in e-commerce, contracts are usually virtual and borderless⁶⁵.

The Law of Contract Act define a Contract as an agreement enforceable by law⁶⁶. Agreement is defined as set of promises⁶⁷ forming consideration. The said agreement may be oral or written, bilateral or unilateral. For that matter therefore, the contract under prescribed formal cannot be valid unless the conditions are fulfilled as it was

⁶¹ Ibid

⁶² CAP 345 R.E. 2019

⁶³ Currently there is no specific Act governing Electronic Transaction Agreements in Tanzania

⁶⁴ Talabi. A., (November 2021) Towards a Robust Consumer Protection Driven Regulatory Framework for E-commerce in Nigeria.. Pg. 30

⁶⁵ See Supra Note 48

⁶⁶ Law of Contract Act. CAP 345 (as amended) S. 2(1)(h)

⁶⁷ Law of Contract Act. CAP 345 (as amended)S. 2(1)(e)

substantiated in *Pandit v. Sekawa*⁶⁸. Contract may be in oral or writing form and it is binding to the contracting parties so long they intend to create legal relationship between them. In Tanzania, it is the presumption of the law that, the same rules in traditional commerce applies mutatis mutandis to e-commerce transactions. The terms for a valid contracts are discussed bellow as follows:

i. Consensus ad idem & Free Consent

The law of Contract Act under section 10⁶⁹ provides that all agreements are contracts provided they have been made from free consent of the parties competent to contract for a lawful consideration with a lawful object. Basically free consent of the parties, lawful subject matter and consideration together with the intention to create legal relations are the main requirements of the contract under the law of contract.⁷⁰ In the famous case of *Star Services Co. Ltd v. Railways Corporation*.⁷¹ The court opined that.

“...the existence of a valid contract presupposes that the contracting parties were ad idem to the terms of the contract and each of them willingly accept those terms...”

This requirement can easily be identified under the traditional agreement where there is a direct meeting of minds because of the access of face to face transactions between the contracting parties but it becomes a challenge when it comes to electronic environment where parties contracts from a distance with no intention of

⁶⁸ 1964 (2) A.L.R Comm.25

⁶⁹ Supra Note 55

⁷⁰ Supra Note 55

⁷¹ (1989)1 HC.

seeing each other, and much more sometimes one or both of the contracting parties are e-agents as referred in the provisions of the law of contract act to a term person⁷². Then this raises the issue on the validity of consent on electronic transactions: whether there is consensus of mind or otherwise. Nevertheless contracting without seeing each other face to face is not a novel method, people in the past used Telegraph⁷³ and they were deemed lawful subject to S. 4⁷⁴ that deems communication complete when it is put in transmission and out of hand of the sender. In the case of *Entores v. Miles Far East*⁷⁵ it was held that ...*telex to be analogous to contracting face to face or over the telephone*. This paves the way for the validity of electronic communication of contracts between parties from distances apart.

i. Intention to Create Legal Relations

In the context of contract law, both parties must have a clear, mutual understanding that they intend their agreement to be legally enforceable and subject to the legal requirements. An agreement is said to be a contract if it has an intention to create legal relations and must be distinguished from social and domestic agreements as set forth in *Jones v. Padavatton*⁷⁶ where the Court held that:

⁷² The Law of Contract Act CAP 345 R.E 2019. S. 2 & 134

⁷³ Telegraph is the long distance transmission of messages where a sender uses symbolic codes, known to the recipient, rather than a physical exchange of an object bearing the message – Wikipedia

⁷⁴ Supra 40 states that "All agreements are contracts if they are made by the free consent of parties competent to contract, for a lawful consideration and with a lawful object and are not hereby expressly declared to be void."

⁷⁵ (1955) 2 QB 327 (CA).

⁷⁶ 3 [1969] 1 WLR 328 Court of Appeal. In this case Plaintiff, a mother of defendant promised defendant to pay her \$ 200 per month for the purpose that her daughter left her job and go to London for bar study. The earlier plan was failed after defendant discovered the said amount was less than she expected and would only afford to rent one room for her and her son. Plaintiff then decided to buy a house for her daughter to live in and rent out some rooms and the income to be used for her

“...the agreement was purely a domestic agreement which raises a presumption that the parties do not intend to be legally bound by the agreement...”

It is the presumption of the law, that, the electronic contract contracted between parties manufacture an intention to create a legal relation between them to obtain protection of the law.

ii. Offer and Acceptance

An offer includes any statement express to do or abstain from doing something with a view to obtain an assent of the other to do or abstain.⁷⁷ This means any statement can be termed as an offer if it entails terms which intend to establish legal obligation against the person who made it as it was celebrated in the case of *Carlill v. Carbolic Smoke ball Company*⁷⁸. Therefore an offer would depends on specific case provided it expresses a reasonable term that intends to establish legal relationship.

Nonetheless an offer should be separated from an invitation to treat; for instance advertisement for sale or display of goods in shop shelves, as it was in the case of *Pharmaceutical Society of Great Britain v Boots Cash Chemists*⁷⁹ where it was held that *the display of goods did not constitute an offer*. On the other hand the law requires offer to be in clear terms⁸⁰. There must be an intention to be bound by the

maintenance. The daughter got married and did not complete the study. Her mother sued for the possession of the house. See also *Ford Motor Co. Ltd v AEF*, 1 WLR 339, 1969

⁷⁷ Supra Note 55

⁷⁸ (1893)1 QB 256. where the court held that plaintiff sued defendant for his advertisement that anyone who will still succumb to influenza after using defendant medicine according to instructions for a fixed period would be offered 1000 pounds, and Court rendered it to be a valid offer.

⁷⁹ 7 (1953)1 QB 401

⁸⁰ Cap.345,R.E 2019. Section 38(2)

parties. An offer should also be distinguished from an invitation to treat⁸¹ and advertisement although some of the advertisement can be treated as offer as it was decided in *Carbolic* case (supra Pg. 27).

Coming on the other part of agreement, acceptance. It is defined an assent to the offer whereby under section 2(b) of the Act⁸² that is to say offerees' assent must be communicated to the offeror according to the terms of the offer.⁸³ It should be unconditionally and when acceptance indicates new terms to an offer it should be taken as counter offer subject to acceptance as it rebuff the original proposal. Additionally silence will not mean acceptance as decided in the case of *Felthouse v Bindley*⁸⁴. However sometimes an offer can be by performance as in the *Carbolic case* (supra Pg. 27)⁸⁵ whereby an offer was made to the public and its acceptance was by the way of performance as illustrated in *Stella Masha v. Tanzania Oxygen Limited*⁸⁶ Whereby the court held that:

“...in order for an acceptance to constitute an agreement, it must in every respect meet and correspond with the terms and conditions of the offer.”

E-commerce consumers, on the other hand, face a challenge in providing a clear acceptance of offers presented to them by online vendors. Challenges arise due to the

⁸¹ *Fisher v Bell* [1961] 1 QB394. where it was held goods on display in shops are not offers but an invitation to treat.

⁸² Cap 345, R.E 2019. “when the person to whom the proposal is made signifies his assent thereto the proposal is said to be accepted”.

⁸³ *Ibid*

⁸⁴ [1862] EWHC CP J35 Court of Common Pleas. Whereby there was an offer made to purchase a horse on condition that if the offeror is not heard from by the weekend offeror would consider the horse to be his. Court held that there was no contract. Silence cannot be acceptance

⁸⁵ *Supra Note 71*

⁸⁶ (2003) TLR 64

distance between the parties involved and the potential defects in goods that might be delivered to the customer in the end.

Contracts in the digital environment introduce various complexities due to the unique characteristics and challenges posed by the digital realm. The formation of a contract typically requires an offer and acceptance. In the digital environment, determining whether an offer has been made and whether acceptance has been communicated can be challenging.⁸⁷ Communication may occur through electronic means, such as emails, instant messaging, or online platforms. Issues can arise regarding the timing, revocability, and reliability of these communications, leading to uncertainties in contract formation.⁸⁸ Another aspect is Digital contracts often involve clickwrap and browsewrap agreements, where users are required to accept terms and conditions to access or use digital services. Clickwrap agreements require users to actively click or check a box to indicate their acceptance. Browsewrap agreements, on the other hand, display terms and conditions on a website without requiring explicit acceptance.⁸⁹ The enforceability of these agreements can be complex, as courts may scrutinize the prominence, clarity, and user awareness of the terms to determine their validity.⁹⁰

Digital platforms may offer services or incentives that require users to perform specific actions to accept the terms. These are known as unilateral contracts.

⁸⁷ Bix, B (2012). Contracts in the Virtual World. *Chicago-Kent Law Review*, 87(3), 805-822 Pg. 806

⁸⁸ Feinman, J. M. (2019). Offer and Acceptance in the Digital Economy. *Mississippi Law Journal*, 88(4), 605-651 Pg. 613

⁸⁹ Loos, M (2016). Standard Terms and Conditions in the Digital Era. In M. B. M. Loos & A. Luzak (Eds.), *Towards a Theory of Legal Uncertainty in Consumer Law* (pp. 189-209). Pg 197

⁹⁰ *ibid.*, Pg. 198

Challenges arise in determining whether the user's actions constitute acceptance and whether the terms of the contract are clear and effectively communicated.⁹¹ The dynamic nature of digital platforms, where terms can change or be updated, adds further complexity.⁹² Also Digital contracts may involve interactions with automated systems or algorithms, such as smart contracts or artificial intelligence-based platforms.⁹³ Issues may arise regarding errors or biases in algorithms, accountability for decisions made by automated systems, and the need for human intervention or oversight,⁹⁴ as in the case of the case of *Cullinane v. Uber Technologies, Inc.*,⁹⁵ where the court had to determine whether an arbitration clause in Uber's terms of service was enforceable against a user who had not physically signed the agreement, but had rather interacted with Uber's mobile app. The Court decided that “merely signing up for an Uber account and using the service did not constitute explicit acceptance of the arbitration clause. More affirmative action was required from the user”. Digital contracts often involve the collection, processing, and sharing of personal data. Compliance with data protection and privacy laws, can be complex.⁹⁶

Consumers may face challenges in understanding and accessing the terms and conditions of digital contracts as in the case of the case of *Nguyen v. Barnes & Noble Inc.*,⁹⁷ which addressed the issue of how to properly provide notice and obtain consent for contractual terms in a digital environment and where the Court ruled that

⁹¹ Ibid

⁹² Ibid. Pg. 199

⁹³ Bix, B. H. Op. Cit., Pg. 811

⁹⁴ Ibid. Pg. 812

⁹⁵ 893 F.3d 53 (1st Cir. 2018)

⁹⁶ Feinman, J. M. Op Cit., Pg. 643

⁹⁷ 763 F.3d 1171 (9th Cir. 2014)

the mere existence of a hyperlink to terms of use is not sufficient to put a reasonably prudent user on notice of those terms. Issues such as unfair contract terms, hidden fees, or misleading information can arise, necessitating robust consumer protection regulations and enforcement mechanisms. In the digital environment, contract performance and enforcement can encounter challenges. Parties may face difficulties in verifying and ensuring the performance of obligations, especially when dealing with remote or international transactions.⁹⁸

2.6 Problems E-commerce Consumer Face in Tanzania

The e-commerce marketplace has changed dramatically over the recent decades, spurred by fast-moving digital innovation and new business models, increased Internet access and mobile connectivity, as well as the rise of online marketplaces as major channels for business-to-consumer and consumer-to-consumer online transactions⁹⁹. However it is with this advancement, comes challenges that put consumers at risks of losing their money and/or time. There are number of legal issues in e-commerce that affects consumer directly. These issues are going to be discussed next as follows;

2.6.1 Security and Privacy Concern

Security and privacy concerns are significant challenges for e-commerce consumers.

Consumers may worry about the safety of their personal and financial information

⁹⁸ Nancy S., Digital Contracts (June 1, 2018 - May 31, 2019) (February 7, 2020). 75 The Business Lawyer 1683 (Winter 2019-2020), Pg. 1 Retrieved from <https://ssrn.com/abstract=3534269> accessed on 31/05/2024

⁹⁹ Report on the Implementation of the OECD Recommendation on Consumer Protection in E-Commerce (2022). Pg. 4

when making online purchases. Issues such as data breaches, identity theft, and unauthorized access to sensitive information can erode consumer trust in online transactions.¹⁰⁰ When engaging in online transactions, consumers entrust sensitive personal and financial information to e-commerce platforms and online retailers¹⁰¹ i.e. information such as name, address, credit or debit card details, gender, birth date, ID, address, phone number and email addresses, personal income, credit card/ debit card details, and other necessary information for the transaction. This has prompted a number of fraudulent activities to e-commerce users as follows:

- a. **Data Breaches:** E-commerce platforms are attractive targets for cybercriminals due to the vast amount of personal information they store. Data breaches can result in unauthorized access to consumer data, including names, addresses, payment card details, and login credentials. This information can be used for identity theft, fraud, or sold on the black market.¹⁰² Privacy invasion usually occurs for two purposes, first to enhance customer satisfaction and to increase profitability. Businesses use the data collected to offer customers customised services or use them for "web lining", this is a situation where users are shown different prices based on the information submitted. Here, the user's profile will determine the price offered; wealthy users are charged more, while those who are not will be charged less¹⁰³.

¹⁰⁰ Mwakatumbula, H. Op Cit., Pg 31

¹⁰¹ Anitesh B, Jon P, Jay S, and Whinston B. (1999), "*Measuring the Internet Economy: An Exploratory Study*," (accessed March 6, 2000), [available at http://cism.bus.utexas.edu/works/articles/internet_economy.pdf].

¹⁰² Talabi. A., (Supra 57)

¹⁰³ Ibid

b. **Identity Theft:** E-commerce consumers are vulnerable to identity theft, where Fraudsters can use the stolen data (like Social Security numbers, addresses and card details) to create a synthetic ID and steal funds from accounts; take out loans; or create new credit lines in the name of the customer.¹⁰⁴ This can lead to financial losses, damaged credit scores, and significant inconvenience for the victims.¹⁰⁵ This has been the main challenge for mobile users in the country to deal with i.e. people with malicious intent would register multiple sim cards only to use them to scam other via messages and false customer care calls. According to the Tanzania Communication Regulatory Authority (TCRA) it recorded 12,044 fraud incident for the period January to March 2023.¹⁰⁶ Though this figure has decreased a little it is still significant. The Regulator asserts that Tigo is leading at 34% of all fraud instances, Airtel comes second with 32% ahead of Vodacom 28% and TTCL 3%.¹⁰⁷ Geographically the Rukwa region is Leading with 45% of all instances, Morogoro is second with 18% while Dar es salaam is third with 14% and followed by Mbeya with 7%.¹⁰⁸

¹⁰⁴Trivedi V. (1 April 2021) E-commerce fraud to surpass \$20B in 2021, an 18% jump over last year, report finds retrieved from <https://www.paymentsdive.com/news/e-commerce-fraud-to-hit-20-billion-2021-an-18-jump-from-prior-year/599312/#:~:text=Fraudsters%20can%20use%20the%20stolen%20data%20%28like%20Social,the%20Federal%20Trade%20Commission%20%28FTC%29%2C%20tracks%20identity-related%20fraud.> Accessed on 1st June 2024

¹⁰⁵ Ibid

¹⁰⁶ DigWatch (April 2023). Fraud incidents decrease in Tanzania, but SIM card scams remain a major concern. Retrieved from <https://dig.watch/updates/fraud-incidents-decrease-in-tanzania-but-sim-card-scams-remain-a-major-concern#:~:text=Fraud%20incidents%20decrease%20in%20Tanzania%2C%20but%20SIM%20card,r egulators%20and%20mobile%20network%20operators%20to%20combat%20it>. Accessed on 1st June 2024

¹⁰⁷ Ibid

¹⁰⁸ ibid

c. **Phishing and Scams:** Phishing attempts involve fraudulent emails, messages, or websites designed to deceive consumers into providing sensitive information. Scammers may impersonate legitimate businesses, requesting login credentials, credit card details, or other personal data. Consumers need to be cautious and verify the authenticity of communication and website addresses to avoid falling victim to such scams (Liu & Liu, 2012). Attackers may use these phishing emails that contain links that directs users to websites which collect personal information such as login credentials, or contain malicious attachment that can infect a system.¹⁰⁹

d. **Lack of Transparency in Data Handling & Tracking and Profiling:**

Consumers may be concerned about how their personal information is collected, stored, and shared by e-commerce platforms.¹¹⁰ Privacy policies should clearly outline how data is handled, whether it is shared with third parties, and the security measures in place to protect consumer information. E-commerce platforms often use tracking technologies, such as cookies and web beacons, to collect data on consumer behavior, preferences, and browsing activities. Cookies extract information as a consumer browses through the internet.¹¹¹ The e-commerce site usually sends these cookies to the consumer's computer, saving them on the hard drive. Thus, when a consumer revisits the e-commerce site, the site gets a

¹⁰⁹ Ebola Phishing Scams and Malware Campaigns retrieved from <https://www.tzcert.go.tz/ebola-phishing-scams-and-malware-campaigns> accessed on 12 April 2024

¹¹⁰ Ibid

¹¹¹ ThoughtMetric. Cookie: E-Commerce Explained. Understanding Cookies in E-commerce. retrieved from <https://thoughtmetric.io/define/cookie#:~:text=When%20a%20user%20visits%20a%20website%2C%20the%20site,recognize%20the%20user%20and%20provide%20a%20personalized%20experience.> Accessed on 1st June 2024

notification. In addition, these cookies monitor the consumer's activities on the website by studying the consumer's preferences and shopping patterns¹¹²

2.6.2 Jurisdiction & Appropriate Dispute Resolution

Jurisdiction, choice of law, and dispute resolution are significant challenges in the realm of e-commerce. As online transactions transcend geographical boundaries, determining the appropriate jurisdiction and applicable laws becomes complex.¹¹³ Additionally, resolving disputes efficiently and fairly is crucial for maintaining trust and confidence in electronic commerce.¹¹⁴ Let's delve into each of these aspects in more detail:

Jurisdiction: Jurisdiction refers to the authority of a court to hear and decide a case. In traditional brick-and-mortar commerce, jurisdiction is typically determined based on the physical location of the parties or the occurrence of the disputed event.¹¹⁵ However, in e-commerce, the parties involved may be situated in different countries or even different continents. This raises questions like: Which court has the authority to hear the case? Is it the court where the buyer resides, the seller is located, or the server hosting the website is situated? Determining jurisdiction in e-commerce requires careful consideration of various factors, including the parties' locations, contractual agreements, and local laws.¹¹⁶

¹¹² Ibid

¹¹³ Wang, FF., (2010). Internet Jurisdiction and Choice of Law: Legal Practices in the EU, US & China. retrieved from <https://archive.org/details/internetjurisdic0000wang> accessed on 22nd May 2024

¹¹⁴ Ibid

¹¹⁵ Ibid

¹¹⁶ Shaik D., & Poojasree V., (2020). "Consumer Protection in E-commerce: A Legal and Compliance Framework for the Digital Market" 549 *Advances in Social Science, Education and Human Research*.

Choice of Law, the Choice of law refers to the selection of a particular jurisdiction's laws that will govern the contractual relationship between the parties. In e-commerce, selecting the appropriate legal framework is vital for addressing issues such as contract formation, consumer protection, intellectual property rights, and liability. The choice of law can significantly impact the rights and obligations of the parties involved. However, determining the applicable law can be challenging due to the global nature of e-commerce transactions. It often involves analyzing conflicts of law rules and contractual provisions, which may vary across jurisdictions.¹¹⁷

Dispute Resolution: Disputes arising from e-commerce transactions need to be resolved efficiently and effectively to maintain trust and ensure fair outcomes. Traditional dispute resolution mechanisms, such as litigation in courts, can be time-consuming, expensive, and impractical in cross-border scenarios.¹¹⁸ Alternative dispute resolution (ADR) methods, such as arbitration and mediation, offer more flexible and expedited means of resolving e-commerce disputes. These methods allow parties to select neutral decision-makers, establish procedural rules, and achieve enforceable outcomes.¹¹⁹ Integrating ADR mechanisms into e-commerce platforms and contracts can enhance accessibility and streamline the resolution process.

¹¹⁷ Ibid

¹¹⁸ Cortes, P., & Ladder, AP., (2014) "Consumer Dispute Resolution Goes Online: Reflections on the Evolution of European Law for Out-of-Court Redress) 21 Maastricht Journal of European & Comparative Law at 15.

¹¹⁹ Ibid

To address these challenges, several initiatives have been undertaken at the international level. For instance, the United Nations Commission on International Trade Law (UNCITRAL) has developed the UNCITRAL Model Law on Electronic Commerce and the UNCITRAL Model Law on Electronic Signatures.¹²⁰ These model laws provide a framework for harmonizing e-commerce legislation across jurisdictions, facilitating the recognition and enforcement of electronic contracts, and promoting uniform rules for jurisdiction and choice of law.

Furthermore, organizations like the International Chamber of Commerce (ICC) have established rules and guidelines for online dispute resolution (ODR) to provide efficient mechanisms for resolving e-commerce disputes. ODR platforms leverage technology to facilitate communication, negotiation, and decision-making between parties, promoting faster and cost-effective resolutions.¹²¹

Addressing these challenges necessitates international cooperation, the development of harmonized legal frameworks, and the integration of technology-driven dispute resolution mechanisms.¹²² By establishing clear rules and procedures, enhancing cross-border cooperation, and embracing innovative approaches, the e-commerce ecosystem can foster trust, facilitate transactions, and protect the rights of all parties involved.

¹²⁰ UNCITRAL Model Law on International Commercial Arbitration(1994). Retrieved from https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/06-54671_ebook.pdf accessed on 28th March 2024

¹²¹ UNCITRAL Model Law on International Commercial Arbitration https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/06-54671_ebook.pdf accessed on 22nd April 2024

¹²² Ibid

2.7 Theories

Consumer protection in the digital economy is governed by a range of theories and principles designed to ensure that consumers' rights are safeguarded in an increasingly complex and digital marketplace. Here are some key theories and frameworks:

2.7.1 Information Asymmetry Theory

This theory posits that markets function efficiently when all parties have access to relevant information. In the digital economy, there often exists a significant imbalance where businesses have more information about products and services than consumers.

2.7.1.1 Implications for Consumer Protection

Regulations and policies are designed to ensure transparency and that consumers receive accurate, comprehensive, and understandable information about digital products and services. Examples include mandatory disclosure of terms and conditions, clear privacy policies, and product descriptions.

2.7.2 Behavioral Economics:

This theory explores how psychological, cognitive, emotional, cultural, and social factors affect economic decisions. Consumers do not always act rationally and can be influenced by how choices are presented to them.

2.7.2.1 Implications for Consumer Protection

Laws and regulations may require that digital platforms design interfaces that protect consumers from manipulative practices, such as dark patterns, and provide default settings that favor privacy and consumer well-being.

2.7.3 Contract Theory

This theory deals with the design and enforcement of contracts. In the digital economy, standard form contracts (like terms of service) often bind consumers.

2.7.3.1 Implications for Consumer Protection

There is a need for ensuring that these contracts are fair, understandable, and not overly burdensome to the consumer. This includes scrutinizing and potentially regulating terms of service and end-user license agreements.

2.7.4 Market Failure Theory

This theory suggests that markets do not always allocate resources efficiently on their own due to various reasons such as monopolies, externalities, or public goods.

2.7.4.1 Implications for Consumer Protection

Government intervention is justified to correct these failures. In the digital economy, this could mean anti-trust regulations, protection against monopolistic practices, and ensuring competition to benefit consumers.

2.7.5 Rights-Based Approach

This approach focuses on the protection of fundamental rights, such as privacy, freedom of expression, and access to information.

2.7.5.1 Implications for Consumer Protection

Regulations like the General Data Protection Regulation (GDPR) in the EU enforce strict rules on how personal data is collected, stored, and used, thereby protecting consumers' privacy rights.

2.7.6 Fairness and Equity Theory

This theory emphasizes fairness and equitable treatment in transactions. Consumers should not be exploited or treated unfairly.

2.7.6.1 Implications for Consumer Protection

Policies aim to protect vulnerable consumers, prevent discriminatory practices, and ensure that all consumers have access to essential digital services.

2.7.7 Product Liability and Safety

This theory asserts that producers and sellers are responsible for the safety of their products.

2.7.7.1 Implications for Consumer Protection

Digital products and services, including software and hardware, must meet safety standards. Consumers should be protected from defective products and have avenues for redress.

2.7.8 Consumer Empowerment

This approach focuses on enabling consumers to make informed choices and have control over their transactions.

2.7.8.1 Implications for Consumer Protection

Education initiatives, access to comparison tools, and enhanced digital literacy are key to empowering consumers in the digital marketplace.

Each of these theories contributes to a comprehensive framework for consumer protection in the digital economy, guiding the development of laws, regulations, and policies to ensure that consumers can navigate the digital world safely and fairly.

2.8 Conclusion

This Chapter showcased how e-commerce has transformed the way consumer engaged in commercial transactions consequently presented new challenges for consumer protection. To ensure a safe and trustworthy digital marketplace, it is of the essence to address issues such as information asymmetry, trust, security and effective dispute resolution mechanism. By implementing robust legal framework, enhancing transparency, promoting collaboration among stakeholders and and leveraging technological advancement an environment of consumer protection can be fostered.

CHAPTER THREE

**INTERNATIONAL AND REGIONAL INSTRUMENTS REGULATING
CONSUMER PROTECTION IN THE DIGITAL ECONOMY**

3.1 Introduction

The rapid growth of the digital economy has revolutionized the way individuals and businesses interact and conduct transactions. In this era of technological advancement, consumers are increasingly relying on digital platforms and services for various aspects of their daily lives, from shopping and banking to communication and entertainment.¹²³

Recognizing the need to safeguard consumer rights and interests in the digital realm, international and regional instruments have emerged to regulate consumer protection in the digital economy. This chapter focuses on the international and regional instruments that govern consumer protection. By examining the relevant international and regional instruments, this chapter seeks to shed light on the legal and regulatory landscape governing consumer protection in the digital economy in Tanzania.

The chapter will then delve into the key international instruments that Tanzania has ratified or adhered to, such as the United Nations Guidelines for Consumer Protection,¹²⁴ the World Trade Organization (WTO) agreements,¹²⁵ International

¹²³ Ey(2023). How to serve consumers who rely on tech but don't trust tech. Retrieved from https://www.ey.com/en_gl/insights/consumer-products/how-to-serve-consumers-who-rely-on-tech-but-dont-trust-tech#:~:text=Consumers%20are%20increasingly%20relying%20on,or%20reduce%20their%20environmental%20footprint (2nd part) on 17th April 2024

¹²⁴ As adopted by the General Assembly in Resolution 70/186 of 22 December 2015

Consumer Protection and Enforcement Agency (ICPEN), African Union Convention on Cyber Security and Personal Data Protection and the East Africa Community Competition Act 2006. These instruments play a crucial role in setting standards and principles for consumer protection across borders and provide a foundation for domestic legislation and enforcement mechanisms.

3.2 International Instruments Regulating Consumer Protection

A new consumer law framework is emerging at the International level, promoted by international and regional organizations (Durovic and Micklitz 2017) . the landscape has experience dramatic transformation, and consumer have been facing expanding range of challenges. Therefore the need of International bodies to come together to address the challenges arose. International organization have increasingly become involved in the development of consumer protection.¹²⁶

3.2.1 United Nations Guidelines on Consumer Protection (UNGCP)

The United Nations Guidelines on Consumer Protection (UNGCP) serve as a fundamental framework aimed at promoting and safeguarding consumer rights globally.¹²⁷ Established to enhance consumer welfare, these guidelines seek to address the evolving challenges posed by the rapid growth of the digital economy

¹²⁵ Tanzania member since 1 January 1995

¹²⁶ Benohr, I. (2010). the United Nations Guidelines for Consumer Protection: Legal implication and New frontiers. J Consum Policy43, 105-124

¹²⁷ Marques L & Wei(Eds.), (2017). Consumer Law and Social Economic Development: National and International Dimensions. Cham: Springer. Pg. 40-49.

and e-commerce. They emphasize the necessity of protecting consumers from exploitation and ensuring fair treatment in marketplace transactions (Benohr, 2020).

3.2.1.1 Basic Principles of the UNGCP

The UNGCP is built upon several core principles designed to promote consumer protection: Right to Safety: Consumers should be protected against hazards to health and safety.¹²⁸ Right to Information: Consumers have the right to receive adequate and accurate information to make informed purchasing decisions; Right to Choose: Consumers should have access to a variety of products and services at competitive prices; Right to Redress: Consumers should have access to fair and timely compensation for misrepresentation or poor quality goods.¹²⁹ Right to Consumer Education.¹³⁰ Consumers should be educated about their rights and responsibilities.

These principles are particularly significant in the context of the digital economy, where consumers often face challenges related to transparency, security, and data privacy.¹³¹

3.2.1.2 Implementation of the UNGCP

Implementation of the UNGCP varies across countries, often influenced by local legal frameworks and regulatory environments. Countries are encouraged to adopt

¹²⁸ The United Nations Guidelines on Consumer Protection (as expanded) Section IV, Guideline 11(a) to 11(f). 2015.

¹²⁹ The United Nations Guidelines on Consumer Protection (as expanded). Section F, Guideline 39

¹³⁰ The United Nations Guidelines on Consumer Protection (as expanded) Section IV, Guideline 11(d). 2015

¹³¹ The United Nations Guidelines on Consumer Protection (as expanded) Section IV, Guideline 11(b). 2015. also available through https://www.un.org/esa/sustdev/publications/consumption_en.pdf

and adapt the guidelines to fit their unique economic, cultural, and social contexts.

This may involve:

Legislative Actions: Establishing laws that align with the UNGCP principles, ensuring consumer rights are protected in the digital marketplace.¹³²

Institutional Frameworks: Creating or strengthening consumer protection agencies that can enforce regulations and provide support to consumers.¹³³

Awareness Campaigns: Launching initiatives aimed at educating consumers about their rights and available resources.¹³⁴

In Tanzania, the integration of the UNGCP into national policies has been slow, primarily due to existing gaps in consumer protection laws that do not adequately address digital transactions.

3.2.1.3 Challenges in Implementation

Several challenges hinder the effective implementation of the UNGCP: the Guidelines are non binding meaning countries are not obliged to adopt or implement them.¹³⁵

Lack of Awareness: Both consumers and businesses often lack awareness of the guidelines, leading to insufficient adherence to consumer rights.

Insufficient Legal Frameworks: Many countries, including Tanzania, struggle with outdated laws that fail to address the complexities of the digital economy.

Resource Constraints:

¹³² The United Nations Guidelines on Consumer Protection (as expanded) Section I, Guideline 11(a) to (h). 2015

¹³³ The United Nations Guidelines on Consumer Protection (as expanded). Section VII, Guideline 95

¹³⁴ The United Nations Guidelines on Consumer Protection (as expanded) Section IV, Guideline 11(c). 2015

¹³⁵ Talabi, Adetutu (Supra Note 42) Pg. 28

Regulatory bodies may lack the necessary resources and capacity to enforce consumer protection laws effectively. Cross-Border Issues: The global nature of digital transactions complicates the enforcement of consumer protections, as laws vary significantly between jurisdictions.

3.2.1.4 Benefits Achieved

Despite these challenges, there are notable benefits from the UNGCP's implementation: Improved Consumer Awareness: Increased emphasis on consumer education has led to better-informed consumers who are more aware of their rights.¹³⁶ Enhanced Trust in the Digital Market: By promoting fair practices and transparency, the UNGCP contributes to building consumer trust in digital platforms, essential for the growth of e-commerce. Framework for Policy Development: The guidelines provide a robust framework for governments to develop and reform consumer protection legislation, ensuring it remains relevant in the digital age.¹³⁷

In summary, while the UNGCP offers a comprehensive framework for consumer protection in the digital economy, its effectiveness in Tanzania is contingent upon the alignment of national laws with these principles, increased consumer awareness, and the capacity of regulatory bodies to enforce protections effectively.¹³⁸

¹³⁶ The United Nations Guidelines on Consumer Protection (as expanded). Section F, Guideline 37.

¹³⁷ The United Nations Guidelines on Consumer Protection (as expanded). Section J. Guideline 66(d)&(e)

¹³⁸ Talabi, Adetutu (Supra Note 42)

3.2.2 World Trade Organisation (WTO)

The World Trade Organization (WTO) plays a crucial role in shaping international trade rules, which indirectly impacts consumer protection. The rationale behind WTO regulations is to promote free and fair trade among member countries, thereby fostering economic growth and ensuring that consumers benefit from a competitive marketplace.¹³⁹ By establishing a framework for trade, the WTO aims to eliminate barriers that could disadvantage consumers, such as tariffs and quotas, thus enhancing access to a broader range of goods and services.¹⁴⁰

3.2.2.1 Basic Principles of the WTO Instrument

The WTO operates on several core principles that are pertinent to consumer protection: Most-Favored-Nation (MFN) Treatment: This principle requires that any favorable trading terms offered by one WTO member to another must be extended to all other members.¹⁴¹ This ensures that consumers have equal access to products from different countries without discrimination. National Treatment: Once goods have entered a market, they should be treated equally to domestically produced goods.¹⁴² This prevents local businesses from receiving preferential treatment, thereby ensuring that consumers can choose from a diverse range of products.¹⁴³ Transparency: Members are required to publish their trade regulations and practices,

¹³⁹ WTO (2023) Retrieved from https://www.wto.org/English/thewto_e/whatis_e.htm (Para 1) Accessed on 27th February 2024

¹⁴⁰ WTO (2023) Retrieved from https://www.wto.org/English/thewto_e/whatis_e/inbrief_e/inbr_e.htm Accessed on 27th February 2024

¹⁴¹ The General Agreement on Tariffs and Trade (GATT 1947). Article I. Also available on https://www.wto.org/english/docs_e/legal_e/gatt47_01_e.htm Accessed on 27th February 2024

¹⁴² Agreement Establishing the World Trade Organization, 1995. Article II(2).

¹⁴³ The General Agreement on Tariffs and Trade (GATT 1947). Article III.

allowing consumers to be informed about the products available to them and the standards they must meet.¹⁴⁴

Protection of Public Health and Safety: The WTO allows for measures that protect consumers from risks to health and safety, as long as these measures do not constitute unjustifiable barriers to trade.¹⁴⁵

3.2.2.2 Implementation of the WTO Instrument

The implementation of WTO principles occurs through various agreements, such as the Agreement on Technical Barriers to Trade (TBT) and the Agreement on Sanitary and Phytosanitary Measures (SPS).¹⁴⁶ These agreements guide member countries in establishing standards that protect consumers while facilitating trade.¹⁴⁷ Countries are required to notify the WTO about their regulations and standards, which fosters a collaborative approach to consumer protection.¹⁴⁸ However, the effectiveness of these implementations varies significantly between developed and developing nations, often influenced by their economic capabilities and resources.¹⁴⁹

¹⁴⁴ The General Agreement on Tariffs and Trade (GATT 1947). Article X. Also on Agreement on Technical Barriers to Trade (TBT): Article 2.1

¹⁴⁵ The General Agreement on Tariffs and Trade (GATT 1947). Article XXb also on Agreement on the Application of Sanitary and Phytosanitary Measures (adopted 15 April 1994, entered into force 1 January 1995), 1867 U.N.T.S. 493

¹⁴⁶ Agreement Establishing the World Trade Organization, 1995. Article II(1).

¹⁴⁷ Agreement Establishing the World Trade Organization, 1995. Article II(2).

¹⁴⁸ Kim, S. (2017, September 26). The Effectiveness of the World Trade Organization's Dispute Settlement System. *Oxford Research Encyclopedia of Politics*. Retrieved 5 Nov. 2024, from <https://oxfordre.com/politics/view/10.1093/acrefore/9780190228637.001.0001/acrefore-9780190228637-e-536>.

¹⁴⁹ Bahri, A. (2018). "Chapter 1: Developing countries at WTO Dispute Settlement Understanding: strengthening participation: Enabling Developing Countries". In *Public Private Partnership for WTO Dispute Settlement Enabling Developing Countries*. Cheltenham, UK: Edward Elgar Publishing. Retrieved Nov 5, 2024, from <https://doi.org/10.4337/9781786437495.00010>

3.2.2.3 Challenges in Implementation

While the WTO plays a significant role in international trade regulations, it does have some limitation in effectively protecting online consumers. The WTO's jurisdiction is limited to trade related matters between member countries. It does not have direct authority over domestic consumer protection laws and regulations.¹⁵⁰ On the other hand, while the WTO's dispute settlement mechanism provides a means for resolving trade disputes, its enforcement mechanism are limited¹⁵¹ the available remedies typically involve authorized imposition of retaliatory trade measures, which may not directly address the harm caused to individual online consumers or provide adequate compensation for losses suffered.¹⁵² Furthermore, the WTO's primary focus on trade liberalization and ensuring fair competition, rather than specific consumer protection in the online environment.¹⁵³ As a result there may be gaps in addressing issues such as privacy, data protection and cyber security. Lack of Awareness: Consumers in many regions are often unaware of their rights under WTO agreements, which diminishes the effectiveness of the protective measures in place.

3.2.2.4 Benefits Achieved

Despite the challenges, several benefits have emerged from the implementation of WTO principles regarding consumer protection:

¹⁵⁰ Lianos. I., Mantzari.D., Duran.M.G., Darr.A., and Raslan.A.,(2019). The Global Governance of Online Consumer Protection and E-commerce – Building Trust. World Economic Forum. Page 14.

¹⁵¹ Ibid.

¹⁵² The WTO'S Discussions on Electronic Commerce.(January,2017) Analytical Note.

¹⁵³ Supra Note 136.

Increased Market Access: Consumers benefit from a wider variety of goods due to reduced trade barriers, enhancing competition and potentially lowering prices.¹⁵⁴

Enhanced Product Standards: The emphasis on transparency and standardization under WTO agreements encourages countries to adopt better product safety and quality standards, ultimately benefiting consumers.¹⁵⁵

International Cooperation: The WTO framework fosters collaboration among member countries, which can lead to improved consumer protection laws and practices through shared knowledge and resources.¹⁵⁶

In summary, while the WTO's influence on consumer protection is indirect, its principles and agreements significantly shape the landscape of international trade and consumer rights. The ongoing challenge remains in ensuring that these frameworks are effectively implemented, particularly in developing nations, to truly enhance consumer protection in the digital economy.

3.2.3 International Consumer Protection and Enforcement Network (ICPEN)

The International Consumer Protection and Enforcement Network (ICPEN) is a global network of consumer protection authorities from over 70 countries in the world.¹⁵⁷ It aims to enhance cooperation among member countries and promote effective enforcement of consumer protection laws, including those related to online

¹⁵⁴ Supra Note 159

¹⁵⁵ Agreement Establishing the World Trade Organization, 1995. Article V.

¹⁵⁶ Agreement Establishing the World Trade Organization, 1995. Preamble

¹⁵⁷ ICPEN(2023). Protecting consumers worldwide. Retrieved from <https://icpen.org/protecting-consumers-worldwide> on 26 feb 2024

transactions. ICPEN is an excellent example of an informal way to establish a pathway for cooperation among consumer protection authorities and a forum for multistakeholder dialogue¹⁵⁸

ICPEN operates based on several core principles: Cooperation: Member countries collaborate to share information and best practices, enhancing their ability to combat consumer fraud.¹⁵⁹ Consumer Empowerment: The network aims to empower consumers with knowledge about their rights and the tools to seek redress.¹⁶⁰ Harmonization: ICPEN promotes the harmonization of consumer protection laws and practices among member states to create a more predictable and safe environment for consumers Durovic (2020, Pg 136).

ICPEN supports the digital economy Consumer Protection through handling and resolution of cross-border consumer complaints related to online transactions. It provides mechanisms for consumers to report scams, fraudulent practices, and other issues they encounter while conducting online business with companies from other countries.¹⁶¹ ICPEN member countries work together to address these complaints, investigate the alleged violations, and assist consumers in seeking redress. To achieve

¹⁵⁸ Durovic, M. (2020). International Consumer Law. What is it all about? Journal of consumer Policy. Pg 136

¹⁵⁹ Memorandum on the establishment and Operation of the International Consumer protection and Enforcement Network (ICPEN). Article 4.

¹⁶⁰ Memorandum on the establishment and Operation of the International Consumer protection and Enforcement Network (ICPEN). Article 4 (a)-(f).

¹⁶¹ ICPEN (2016). Memorandum_on_the_Establishment_and_Operation_of_ICPEN_2016. Retrieved from <https://icpen.org/sites/default/files/2017-PDF> on 27th February 2024

this, two prevailing instruments are identified for such purpose; the Sweep Actions and development of the internet platform of www.econsumer.gov.¹⁶²

Sweep Actions performed by ICPEN identify suspicious website to be used to prosecute the traders behind such websites by the relevant National Authority or for educational purpose.¹⁶³ ICPEN International Internet Sweeps is a global initiative of National Consumers Agencies with the aim of protecting and securing the confidence of consumers in e-commerce.¹⁶⁴ whereas the Internet platform www.econsumer.gov website enables the easy reporting of the international scams online.

Futhermore, ICPEN facilitates the sharing of information and best practices among member countries.¹⁶⁵ By sharing knowledge and experiences, member countries can enhance their understanding of online consumer protection challenges and develop effective strategies to address them.¹⁶⁶ The Network encourage maintaining regular contact, in particular by means of atleast one annual conference, and exchange of views.¹⁶⁷ The Network further emphasizes on cooperational at an operation level in preventing market malpractices as they arise. Participating Organisation should endeavor to help each other subject to national law.¹⁶⁸

¹⁶² Durovic, M. 2020 (Supra Note 171) Pg. 137

¹⁶³ Ibid

¹⁶⁴ Ibid

¹⁶⁵ ICPEN (2023). Initiatives. Ritrieved from <https://icpen.org/initiatives> visited on 26 feb 2024

¹⁶⁶ Memorandum on the establishment and Operation of the International Consumer protection and Enforcement Network (ICPEN). Article 5(c)

¹⁶⁷ Memorandum on the establishment and Operation of the International Consumer protection and Enforcement Network (ICPEN). Article 5(b).

¹⁶⁸ Memorandum on the establishment and Operation of the International Consumer protection and Enforcement Network (ICPEN). Article 5(d).

Also, ICPEN encourages member countries to cooperate in cross-border enforcement actions. Online consumer protection issues often involve businesses operating in multiple jurisdictions. Through coordinated efforts, ICPEN member countries can share information, conduct joint investigations, and take enforcement actions against fraudulent or deceptive online businesses that operate across borders.¹⁶⁹ This cooperation helps ensure that online consumers are protected regardless of the geographical location of the businesses they interact with.¹⁷⁰

3.2.3.1 Shortcoming of ICPEN

Although ICPEN has a significant number of member countries, it does not include all nations.¹⁷¹ This limited membership means that not all countries are actively participating in the Network's initiatives, which can hinder its effectiveness in tackling global consumer protection challenges.¹⁷² In Addition to that, ICPEN primarily focuses on cross-border consumer protection cases.¹⁷³ However plenty of cases occur within national borders and ICPEN's jurisdiction does not extend to cover these domestic issues.¹⁷⁴ Last but not least, the enforcement capability of member agencies varies widely across different countries.¹⁷⁵ Some consumer protection agencies may have robust legal framework, resources, and enforcement

¹⁶⁹ Memorandum on the establishment and Operation of the International Consumer protection and Enforcement Network (ICPEN). Article 4.

¹⁷⁰ Memorandum on the establishment and Operation of the International Consumer protection and Enforcement Network (ICPEN). Article 17.

¹⁷¹ Memorandum on the establishment and Operation of the International Consumer protection and Enforcement Network (ICPEN). Article 6(b)

¹⁷² Durovic, M. (2020) (Supra Note 171) Pg. 137

¹⁷³ Memorandum on the establishment and Operation of the International Consumer protection and Enforcement Network (ICPEN). Article 4(c)

¹⁷⁴ Durovic, M. (2020) (Supra Note 171) Pg. 137

¹⁷⁵ Ibid.

powers while others lack staff and necessary tools to effectively enforce consumer protection laws.

3.2.4 African Union Convention on Cyber Security and Personal Data Protection

The African Union Convention on Cyber Security and Personal Data Protection aims to establish a comprehensive legal framework to enhance cybersecurity and protect personal data across African nations. In an era where digital transactions are increasingly prevalent, the need for a robust framework to safeguard consumers' rights and privacy has become paramount. This instrument addresses the growing concerns regarding cyber threats, data breaches, and the misuse of personal information, which are critical issues in the context of the digital economy.¹⁷⁶

The Malabo Convention is applicable to all proceedings carried out in the territory of a member state.¹⁷⁷ The convention further applies to any processing, collection, transmission, storage or use of personal data by a natural person, the state, local communities, public or private corporate bodies.¹⁷⁸ The Convention also applies to both automated and manual processing of data contained in or meant to be part of a file.¹⁷⁹ Nonetheless the Malabo Convention is not applicable to data processing undertaken for personal or household activities subject to Article 9(2)(a) of the convention.

¹⁷⁶ Abdulrauf L and Fombad C. (2014). The African Union's Data Protection Convention: A possible cause for celebration of human rights in Africa? Pg. 9

¹⁷⁷ African Union Convention on Cyber Security and Personal Data Protection. Article 9(1)(c).

¹⁷⁸ Ibid .

¹⁷⁹ African Union Convention on Cyber Security and Personal Data Protection. Article 1(b).

The Malabo Convention is relevant to digital economy Consumer Protection in various means such as it establishes a comprehensive legal framework for the protection of personal data ensuring that individuals' personal information is collected, processed and stored in a lawful, transparent and fair manner.¹⁸⁰ This is why it is now customary to for Data Protection instruments to establish a special regime for Data Export.¹⁸¹

In Cyber security the Malabo Convention recognizes the increasing threat of cyber-attacks and aims to enhance cybersecurity across the continent.¹⁸² It promotes the adoption of cybersecurity measures by organisations, including the implementation of adequate technical and organizational safeguards. It establishes guideline for incident reporting, incident response and cooperation between stakeholders in the event of cybersecurity breach.¹⁸³ The Convention further illustrate that, each state party shall undertake to provide leadership for the development of the Cyber Security Culture within its borders.¹⁸⁴ in addition to that each state party shall develop public-private partnership as model to engage industry, the civil society and academia in the promotion and enhancement of a culture of cyber security.¹⁸⁵ The convention also emphasizes on the vitality of member states to establish appropriate institutional mechanism responsible for cyber security governance.¹⁸⁶

¹⁸⁰ African Union Convention on Cyber Security and Personal Data Protection. Article 13, Principle 1-6.

¹⁸¹ Abdulrauf and Fombad, (2014). Op Cit Pg. 17

¹⁸² African Union Convention on Cyber Security and Personal Data Protection. Article 24

¹⁸³ African Union Convention on Cyber Security and Personal Data Protection. Article 25

¹⁸⁴ African Union Convention on Cyber Security and Personal Data Protection. Article 26 (2)

¹⁸⁵ African Union Convention on Cyber Security and Personal Data Protection. Article 26 (3)

¹⁸⁶ African Union Convention on Cyber Security and Personal Data Protection. Article 27 (1)&(2)

In Consumer rights the Malabo Convention recognizes consumers' rights in digital environment, including the right to access, rectify, and delete their personal data.¹⁸⁷ It prohibits the unauthorized or unlawful processing of personal data, ensuring that consumers have control over their personal information.¹⁸⁸ It promotes transparency and accountability by requiring organizations to provide clear and concise information about their data practices, including privacy policies and term of service.¹⁸⁹

Also, the Malabo Convention addresses the challenges of cross-border data flows, recognizing that personal data often crosses borders in the digital age. It establishes rules for the transfer of personal data outside of the African Continent, ensuring that adequate safeguard are in place to protect the data.¹⁹⁰ It promote international cooperation and mutual assistance between African Countries to effectively enforce and implement the convention. For the enhancement of its objectives the Malabo convention emphasizes the importance of capacity building in the areas of cyber security and data protection. It encourages member state to develop and implement national cybersecurity and data protection strategies, policies, and legislation.¹⁹¹ It supports the sharing of knowledge, expertise, and resources among countries to enhance their abilities to protect consumers rights in the digital age.¹⁹²

3.2.4.1 Shortcoming of the Malabo Convention

The Malabo Convention is a witness that Africa as a whole has come to terms with the realities of the digital age by confronting emerging human rights challenges.

¹⁸⁷ African Union Convention on Cyber Security and Personal Data Protection. Article 19.

¹⁸⁸ African Union Convention on Cyber Security and Personal Data Protection. Article 13 part 1

¹⁸⁹ African Union Convention on Cyber Security and Personal Data Protection. Article 16.

¹⁹⁰ African Union Convention on Cyber Security and Personal Data Protection. Article 26 part 6(a)

¹⁹¹ African Union Convention on Cyber Security and Personal Data Protection. Article 26 (4)

¹⁹² African Union Convention on Cyber Security and Personal Data Protection. Article 28 (3)

Nonetheless the Convention still poses a number of issues that may hinder effective realization of the objective of the convention. These problems can be explained as follows:

First, and foremost, the convention itself is extremely broad in scope. According to (Abdulrauf and Fombad, 2014. Pg. 19) the convention is a commercial at the same time, human rights and criminal instrument. The incorporation of these various subject matters into a single legal document has implications for the effective structuring of the document. Further to that, cybercrime often transcends national boundaries, requiring robust international cooperation to combat it effectively. While the convention encourages cooperation among member states, it does not explicitly address cooperation with non member states or international organisations.¹⁹³ Enhancing collaboration with external entities and aligning efforts with other international frameworks could strengthen the convention's impact.¹⁹⁴

3.2.5 The East Africa Community Competition Act, 2006

The East Africa Community Competition Act, 2006 is a significant piece of legislation enacted by the East Africa Community (EAC) to promote fair competition and protect consumers within the member state of the regional bloc. Given the

¹⁹³ Kaaniru J. (2023). The African Union Convention on Cyber Security and Personal Data Protection. Retrieved from <https://cipit.org/the-african-union-convention-on-cyber-security-and-personal-data-protection-key-insights/> para 14. Accessed on 22nd April 2024.

¹⁹⁴ Ibid

¹⁹⁴ Ibid

increasing digitization of markets, the Act seeks to address challenges posed by digital platforms, ensuring that consumers are protected from monopolistic behaviors and unfair trade practices. It forbids unfair trade practices, false or misleading advertising, and deceptive conduct that could harm consumers.

The Act was developed with the objective of enhancing economic integration, fostering market efficiency, and safeguarding consumer welfare.¹⁹⁵ It recognizes the importance of competition in driving innovation,¹⁹⁶ efficiency and productivity in markets, ultimately benefiting consumers and promoting economic growth.¹⁹⁷ By addressing anti-competitive practices, abuse of dominant positions, and regulating mergers and acquisitions, the East Africa Community Competition Act aims to create a competitive and dynamic business environment, protect consumer interests, and contribute to the economic development and integration of the Community member States.¹⁹⁸

Basic Principles of the Instrument

The Act is founded on several key principles: (1) Promotion of Fair Competition: It aims to prevent practices that restrict competition, such as cartels and abuse of dominant positions.¹⁹⁹ (2) Consumer Protection: By ensuring competitive markets, the Act indirectly protects consumers from inflated prices and poor-quality goods

¹⁹⁵ The East Africa Community Competition Act, 2006. Section 3(a).

¹⁹⁶ The East Africa Community Competition Act, 2006. Section 3(b).

¹⁹⁷ The East Africa Community Competition Act, 2006. Section 3(c).

¹⁹⁸ The East Africa Community Competition Act, 2006. Section 3(e).

¹⁹⁹ The East Africa Community Competition Act, 2006. Section 5(1).

and services.²⁰⁰ (3) Regional Cooperation: The Act encourages collaboration among member states in enforcing competition laws and sharing information on anti-competitive practices.²⁰¹

Furthermore the Act has incorporated consumer protection provisions to safeguard the interests of consumers.²⁰² It prohibits deceptive marketing practices, false advertising, unfair trade practices, and the supply of unsafe or substandard goods and services.²⁰³ These provisions aim to ensure that consumers receive accurate information, have access to safe products and services and are protected from fraudulent or unfair business practices.

The Act as well empowers the competition authority to conduct market investigation and inquiries to assess the state of competition in specific sectors or markets.²⁰⁴ This enables the authority to identify any anti-competitive behavior, market failure or consumer harm. The finding from these investigations can lead to corrective measures, such as imposing fines, issue warnings or recommending policy changes to protect consumer interests.²⁰⁵

Finally the Act encourages collaboration between the competition authority and other consumer protection agencies within the EAC member States.²⁰⁶ This cooperation

²⁰⁰ The East Africa Community Competition Act, 2006. Section 12(2)

²⁰¹ The East Africa Community Competition Act, 2006. Section 28

²⁰² The East Africa Community Competition Act, 2006. Section 28

²⁰³ The East Africa Community Competition Act, 2006. Section 31(1).

²⁰⁴ The East Africa Community Competition Act, 2006. Section 42(2)(a).

²⁰⁵ The East Africa Community Competition Act, 2006. Section 42(2)(c)&(d).

²⁰⁶ The East Africa Community Competition Act, 2006. Section 42(1)&(2)(g).

ensures a comprehensive approach to consumer protection, leveraging the expertise and resources of relevant agencies to address consumer concern effectively. It is important to note that the effectiveness of the Act in protecting consumers depend on its implimentantion and enforcement by the competition authority of the member state.²⁰⁷

3.2.5.1 Challenges of Implimenting the Act

While the Act plays a significant role towards promoting fair competition and consumer welfare within the East Africa community, it still exhibits certain shortfalls that can affect its effectiveness. The shortfalls are explained down here below;

First and foremost, the Act was enacted in 2006, and since then, market dynamics and technological Advancements have rapidly evolved. The can not fully capture emerging challenges relating to digital markets, platform economies, and new business models. In addition to that the Act faces the challenge of limited enforcement capacity of the East African Competition Authority and National Competition Authorities within member states.²⁰⁸ Likewise limited awareness and understanding of the Act's provisions among businesses, consumers and even some government officials undermines the Acts effectiveness. Addressing these challenges requires concerted effofts from the Eeast Africa Competition Authorities and all related departments.

²⁰⁷ Kilenga,(2023). Op Cit Pg. 10

²⁰⁸ Security and Trust in Africa's Digital Financial Inclusion Landscape retrieved from <https://carnegieendowment.org/2024/03/08/security-and-trust-in-africa-s-digital-financial-inclusion-landscape-pub-91932> Accessed on 8th March,2024

3.3 Recommendations basing on International and Regional Instruments

The government should review existing laws, policies and practices on surveillance, biometric data collection, encryption and data localization to ensure they comply with the data protection principles in the Guidelines by the African Union Convention on Cyber Security and Personal Data Protection. Under the Data Protection law, Tanzania should establish an independent data Protection Authority that is not answerable to another statutory body and whose leaders are appointed through a transparent and competitive process.

Also, Civil society actors should increase its effort to document violation of the right to privacy and use them for awarenesscreation and advocacy for progressive data governance practices. On the other hand, technology companies and other data controllers should implement privacy and data protection policies and best practices in their handling of consumers data. Lastly is by establishing an efficient and accessible Online Dispute Resolution mechanism to help speed and resolve consumer disputes in e-commerce. the system will facilitate fast and cost effective resolution of disputes, promoting trust and confidence in online transaction.

3.4 Conclusion

The chapter has revealed that the regime of digital market consumer protection worldwide and Tanzania in particular has introduced various legal and regulatory challenges that need to be resolved. In order to harmonise the situation in the country, the guidelines provided by the international standard setting bodies and model laws have proved to be very useful in the making of legal framework for

digital market consumer protection. For example Tanzania adopted the UNICITRAL model law and SADC model law in the construction of the Electronic transaction Act of 2015. By considering the international instruments regarding digital market consumer protection, the legal and regulatory framework that can best fit in the current situation.

CHAPTER FOUR
EXPERIENCE FROM OTHER JURISDICTION: LESSON FOR
TANZANIA

4.1 Introduction

In the current global economy, with highly concentrated markets, competition policy is even more relevant to create an enabling business environment and provide opportunities for start-ups and small and medium-sized enterprises²⁰⁹. As business and consumers increasingly engage in online commerce it becomes imperative to examine experiences from other jurisdictions, that have significant strides in e-commerce consumer protection. Kenya and South Africa have demonstrated commendable efforts in recognizing the unique challenges posed by the digital economy and enacting legislation to safeguard consumer interests. This chapter explores the legal framework and regulatory mechanism implemented in Kenya and South Africa to address e-commerce and consumer protection. It explores Consumer Rights and Practices and challenges and future outlooks.

4.2 Kenya

Consumer protection, the institutional framework, and practices in the digital economy in Kenya have seen significant development and progress.²¹⁰ The country has taken substantial steps to establish a comprehensive framework for consumer

²⁰⁹ UNCTAD. Competition and Consumer Protection Policies and Frameworks. Retrieved from https://unctad.org/system/files/official-document/tc2015d1rev2_S03_P02.pdf. Accessed on 1st June 2024

²¹⁰ Abdulrauf, L. and Fombad, C. (2014). Op Cit Pg. 202

protection in the digital sphere. Here is an overview of the current situation regarding consumer protection in the digital economy in Kenya:

4.2.1 Kenya Legal Framework

The Kenyan Constitution of 2010²¹¹ includes provisions that protect consumer rights, including the right to fair information, protection from unfair trade practices, and the right to consumer education. It is therefore compulsory to pass laws that protect consumer affairs. Kenya has specific legislation and regulations that address consumer protection in the digital economy. This includes laws on electronic transactions, electronic signatures, consumer rights in online transactions, and protection against cybercrime.²¹² These laws are:

4.2.1.1 Communications (Electronic Transactions) Regulations, 2009

The Communications (Electronic Transactions) Regulations, 2009 were established to create a legal framework that facilitates electronic transactions while protecting consumers in the digital marketplace. The rapid adoption of digital technologies and e-commerce necessitated regulations that address issues such as authentication, data integrity, and consumer rights. The rationale behind these regulations is to enhance the legal recognition of electronic transactions, thereby fostering confidence among consumers and businesses in engaging with digital platforms.²¹³

²¹¹ Supreme law of the Republic of Kenya and binds all persons and all state organs at both levels of Government

²¹² Ibid

²¹³ Communications (Electronic Transactions) Regulations, 2009. R. 8(5)

The Regulations are based on several key principles: (1) Legal Recognition of Electronic Transactions: Establishing that electronic signatures and records have the same legal standing as their paper counterparts.²¹⁴ (2) Consumer Protection: Ensuring that consumers are informed about their rights and that businesses are held accountable for compliance with the regulations.²¹⁵ (3) Data Security and Privacy: Mandating that businesses implement adequate measures to protect consumer data from unauthorized access and breaches.²¹⁶ The regulations further establish rules for the creation, storage, and retention of electronic records in electronic transactions.²¹⁷ They also require organizations to provide clear and accurate information about their products and services in electronic transactions, including pricing, terms and conditions, and refund policies.²¹⁸

4.2.1.2 The Small Claims Court Act, Cap 10A (R.E. 2002)

The Small Claims Court Act was established to provide a simplified and expedited mechanism for resolving minor disputes, particularly those involving consumer claims. The rationale behind this Act is to make justice accessible for individuals who may not have the resources or ability to navigate the formal judicial system for small claims. By creating a dedicated forum for such disputes, the Act aims to enhance consumer protection, offering a timely resolution to issues related to goods

²¹⁴ Communications (Electronic Transactions) Regulations, 2009. R. 7(2)

²¹⁵ Communications (Electronic Transactions) Regulations, 2009. R. 14(4)

²¹⁶ Communications (Electronic Transactions) Regulations, 2009. R. 16(1)

²¹⁷ Communications (Electronic Transactions) Regulations, 2009. R. 7(1)

²¹⁸ Communications (Electronic Transactions) Regulations, 2009. R. 8(1)

and services..²¹⁹ The Small Claims Court deals with a wide range of disputes, including but not limited to contractual matters, debts, property damage, landlord-tenant disputes, consumer complaints, and professional negligence claims.²²⁰ The Act emphasizes a simplified procedure that encourages parties to represent themselves without the need for legal representation.²²¹ The Act encourages the use of mediation and conciliation to resolve disputes in a non-adversarial manner.²²²

4.2.1.3 The Competition Act

The Competition Act was enacted to promote fair competition and prevent anti-competitive practices in the marketplace.²²³ The rationale behind this legislation is to protect consumers from monopolistic behaviors and unfair trade practices that can lead to higher prices, reduced choices, and substandard goods and services.²²⁴ By fostering a competitive environment, the Act aims to enhance consumer welfare and stimulate economic growth while primarily focused on competition issues, the Act establishes mechanisms for redress and dispute resolution, and promotes consumer education and awareness.²²⁵

²¹⁹ The Small Claims Court Act, Cap 10A (R.E. 2002). S. 12(4).

²²⁰ The Small Claims Court Act, Cap 10A (R.E. 2002). S. 12(1)(a)-(e).

²²¹ The Small Claims Court Act, Cap 10A (R.E. 2002). S. 20(1)&(3).

²²² The Small Claims Court Act, Cap 10A (R.E. 2002). S. 18.

²²³ The Competition Act. No. 12 of 2010. S. 21

²²⁴ The Competition Act. No. 12 of 2010. S. 60.

²²⁵ The Competition Act. No. 12 of 2010. Part VII

4.2.1.4 The Consumer Protection Act

Is a key legislation that specifically focuses on protecting consumer rights and interests across various sectors, including e-commerce.²²⁶ The Act provides a comprehensive framework for ensuring fair and transparent business practices,²²⁷ promoting consumer welfare, and addressing specific challenges faced by e-commerce consumers.²²⁸ It requires e-commerce businesses to provide clear descriptions, specifications, pricing, terms and conditions, and any other relevant information that enables consumers to make informed decisions.²²⁹ Furthermore it prohibits misleading or deceptive conduct, false claims, false advertising,²³⁰ and unfair contract terms.²³¹ The Act establishes mechanisms for consumer redress in cases of disputes or grievances arising from e-commerce transactions.²³² Moreover the Act mandates the Consumer Protection Advisory Committee to promote consumer education programs and campaigns to enhance consumer awareness, knowledge, and understanding of their rights and responsibilities in e-commerce transactions.²³³

4.2.1.5 The Data Protection Act of 2019

Establishes regulations for data protection and privacy, which are crucial in the digital economy. The Data Protection Act of 2019 establishes regulations for the

²²⁶ Act No. 46 of 2012

²²⁷ The Consumer Protection Act. No. 46 of 2012. S. 3(4)(a).

²²⁸ The Consumer Protection Act. No. 46 of 2012. S.3(4)(c).

²²⁹ The Consumer Protection Act. No. 46 of 2012. S. 31 & 87.

²³⁰ The Consumer Protection Act. No. 46 of 2012. S. 15(1)-(3).

²³¹ The Consumer Protection Act. No. 46 of 2012. S. 16(1)-(13).

²³² The Consumer Protection Act. No. 46 of 2012. Part IX.

²³³ The Consumer Protection Act. No. 46 of 2012. S. 90(e)

collection, processing, storage,²³⁴ and use of personal data. The Office of the Data Protection Commissioner (ODPC) oversees the implementation and enforcement of data protection regulations.²³⁵ The Act gives effect to Article 31(c) and (d) of the Constitution of Kenya right to privacy. In addition to that, the Act forbid transfer of data outside Kenya, unless there is proof of adequate data protection safeguards or consent from the data subject.²³⁶ Further to that, the Act confers rights to data subject to object, correct or delete false or misleading data about them.²³⁷ the Act also establishes the conditions for the transfer of data outside of Kenya to be within the limit of the Act.²³⁸ Moreover it establishes a redress mechanism for unsatisfied data subject²³⁹ and confer the power to investigate and enforce decision to the Data Commissioner.²⁴⁰

4.3 South Africa

South Africa has done a commendable job in providing a robust legal and regulatory framework for the protection of consumers under e-commerce. The principal laws regulating e-commerce in South Africa are the Protection of the Personal Information Act, the Electronic Communications and Transactions Act, and the Consumer Protection Act and its Code. This study will outline how these laws protects e-commerce consumers.

²³⁴ The Data Protection Act. No. 24 of 2019. S. 25.

²³⁵ The Data Protection Act. No. 24 of 2019. S. 5

²³⁶ The Data Protection Act. No. 24 of 2019. S. 25(h).

²³⁷ The Data Protection Act. No. 24 of 2019. S. 26.

²³⁸ The Data Protection Act. No. 24 of 2019. S. 48.

²³⁹ The Data Protection Act. No. 24 of 2019. S. 56(1)

²⁴⁰ The Data Protection Act. No. 24 of 2019. S. 57(1)

4.3.1 The Protection of Personal Information Act 2013 (POPIA)

South African has enacted the POPIA to facilitate the protection of citizens' data by providing minimum requirements for collecting, processing, storing, and sharing personal data.²⁴¹ The rationale behind POPIA is to provide a legal framework that ensures the responsible processing of personal data, protecting individuals from misuse, unauthorized access, and breaches of privacy. As digital transactions and online services become commonplace, the need for robust data protection measures has become increasingly critical to maintain public trust and consumer confidence in digital environments. The Act provides for data to be processed lawfully,²⁴² the right to be notified where their data is collected for processing,²⁴³ the right to object to their data being processed,²⁴⁴ the right to file complaints to a regulator²⁴⁵ or institute an action,²⁴⁶ where their rights under the Act have been breached.

The Act establishes the Information Registrar as the body responsible for implementing the act.²⁴⁷ It is responsible for educating the populace on data protection and ensuring compliance with the Act's provisions.²⁴⁸ In addition, the Act mandates the Information Registrar to establish an enforcement committee responsible for the determination of issues arising from the breach of the provisions

²⁴¹ The Protection of Personal Information Act 2013, S. 2

²⁴² The Protection of Personal Information Act 2013, S. 5

²⁴³ The Protection of Personal Information Act 2013, S 5(a)

²⁴⁴ The Protection of Personal Information Act 2013, S. 5 (e)

²⁴⁵ The Protection of Personal Information Act 2013, S. 5 (h)

²⁴⁶ The Protection of Personal Information Act 2013, S. 5 (i)

²⁴⁷ The Protection of Personal Information Act 2013, S. 39

²⁴⁸ The Protection of Personal Information Act 2013, S. 40(1)(a)

of the Act.²⁴⁹ The Act allows data subject to submit its complaints to the Information Registrar for breach of their privacy rights.²⁵⁰ The Act permits the Information Registrar to refer the complaints to other agencies where the Information Regulator believes the complaint is within the expertise of another agency.²⁵¹ Organisations has a duty to appoint an Information Officer that will encourage compliance with the Act within the organisation.²⁵²

4.3.2 The Electronic Transactions and Communications Act 2002 (ETCA)

This law was enacted in 2002 due to the rapid growth of electronic transactions within the country. The ETCA recognises electronic contracts and signatures as having the same legal status as their traditional equivalent.²⁵³ Therefore, businesses are obliged to disclose its legal name, physical address, emails and membership organisation.²⁵⁴ Further to that, businesses are required to give consumers the opportunity to review the entire transaction and correct mistakes before completing the transaction.²⁵⁵ The Act makes it compulsory for businesses to use secure payment methods in line with the minimum standards required in South Africa unless otherwise, it will be liable for any loss suffered by the consumer.²⁵⁶ The Act also provides for the protection for the storage and processing of consumers' data.²⁵⁷

²⁴⁹ The Protection of Personal Information Act 2013, S. 50

²⁵⁰ The Protection of Personal Information Act 2013, S. 74

²⁵¹ The Protection of Personal Information Act 2013, S. 78.

²⁵² The Protection of Personal Information Act 2013, S. 92

²⁵³ Electronic Transactions and Communications Act, S. 13

²⁵⁴ Electronic Transactions and Communications Act, S. 43

²⁵⁵ Electronic Transactions and Communications Act, S. 43(2)

²⁵⁶ Electronic Transactions and Communications Act, S. 43(6)

²⁵⁷ Electronic Transactions and Communications Act, S. 49

moreover, it makes provision for cybercrimes²⁵⁸ and the appointment of cyber inspectors to implement the provisions on cybercrimes.²⁵⁹ Under the ETCA, consumers have a "cooling off" period where they are allowed to cancel a transaction without reason²⁶⁰ subject to the Act's conditions.²⁶¹ In addition, where a consumer has already made a payment, the consumer is entitled to a refund within 30 days from the date of cancellation.

4.3.3 The Consumer Protection Act 2008

The South Africa Consumer Protection Act (CPA) was enacted to protect both traditional and online consumers. The CPA recognises the idiosyncrasies of online transactions, thus, it provides that issues such as the delivery rights of consumers and cooling of periods for online consumers.²⁶² the CPA, provides further that, delivery must be done at the time agreed. Unlike the previous Act in (4.3.2), the cooling period under the CPA is five days.²⁶³ Nevertheless The CPA establishes the National Consumer Commission responsible for the implementation of its provisions.²⁶⁴ The CPA also provides a plethora of options for consumers to seek redress. Consumers can seek redress by filing complaints to the Commission or the Tribunal on

²⁵⁸ Electronic Transactions and Communications Act, S. 85

²⁵⁹ Electronic Transactions and Communications Act, S. 81

²⁶⁰ Electronic Transactions and Communications Act, S. 44

²⁶¹ Electronic Transactions and Communications Act, S. 44(1)(b)

²⁶² The Consumer Protection Act 2008, S. 16

²⁶³ Ibid

²⁶⁴ The Consumer Protection Act 2008, S. 85

Consumer Protection directly.²⁶⁵ Consumers can also explore Alternative Dispute Resolution Mechanisms such as Mediation, Conciliation or Ombudsmen.²⁶⁶

To deal with consumer problems, South African government has established the Consumer Goods and Services Ombud (CSGO)²⁶⁷ to receive complaints, carry out investigations and make recommendations. Such recommendations will be submitted to the Consumer Tribunal or a High Court to convert this into a consent judgment where the parties agree. The CGSO can also conduct mediation where the parties agree for this to happen. They are also to refer complaints that can be dealt with more appropriately by other agencies.²⁶⁸

4.4 Conclusion

Kenya and South Africa have made significant progress in establishing a comprehensive framework for consumer protection in the digital economy in Africa. The two countries have specific legislations, institutions, and practices in place to protect consumers in online transactions. However, on-going efforts are needed to strengthen enforcement mechanisms, enhance cyber security measures, and adapt to technological advancements to ensure robust consumer protection in the digital sphere.

²⁶⁵ The Consumer Protection Act 2008, S. 69

²⁶⁶ The Consumer Protection Act 2008, S. 70

²⁶⁷ The Consumer Protection Act. 2008, S. 82(6)

²⁶⁸ Consumer Goods and Service Ombud. About Us. Retrieved from <https://www.cgso.org.za/cgso/about-us/> Accessed on 2nd June 2024

CHAPTER FIVE
LEGAL FRAMEWORK GOVERNING DIGITAL ECONOMY IN
TANZANIA

5.1 Introduction

The digital economy has become a significant driver of economic growth and innovation in Tanzania and worldwide at large.²⁶⁹ As technology continues to grow and transform traditional industries, it is crucial to establish a robust legal, strategies and regulatory framework to govern the digital economy. This chapter aims to explore the strategies, policy and legal landscape governing the digital economy in Tanzania *i.e.* Legislation Policies and Strategy related to Data Protection and privacy, electronic transactions, cybersecurity, competition and consumer protection. Further to that, this chapter will explore the roles and responsibilities of regulatory bodies and agencies involved in digital economy.

5.2 Tanzania Legal Framework

The right of consumer protection are primarily enshrined in the Constitution of the country.²⁷⁰ The Constitution provides for the right to; fair treatment, right to information, healthy and safety, right to redress and right to privacy.²⁷¹ It is therefore compulsory to pass laws that protects consumer affairs. Tanzania has made huge step in passing laws that protects consumers. It is therefore compulsory to pass laws that protects consumer affairs. In Tanzania these laws are:

²⁶⁹ Mzurikwao A. (2018). Op Cit Pg. 84

²⁷⁰ The Constitution of United Republic of Tanzania. CAP 2. 1977 (as amended)

²⁷¹ The Constitution of United Republic of Tanzania. CAP 2. 1977 (as amended). Part III

5.2.1 The Electronic Transactions Act No.13 of 2015

The Electronic Transactions Act No. 13 of 2015 was enacted to provide a legal framework for electronic transactions in Tanzania, reflecting the growth of digital commerce and the need for a regulatory environment that supports it.²⁷² The rationale behind this legislation is to ensure that electronic transactions have the same legal standing as traditional paper-based transactions, thereby fostering confidence among consumers and businesses in using digital platforms.²⁷³ This Act aims to address issues such as authentication, data integrity, and consumer rights, facilitating the growth of the digital economy.²⁷⁴ Nonetheless Many consumers and businesses may not fully understand the provisions of the Act, which can limit its effectiveness in protecting rights and ensuring compliance. Second, Regulatory bodies face challenges related to staffing and funding, affecting their ability to monitor compliance and enforce the Act effectively. Third, The fast pace of technological advancements in digital transactions create gaps in the regulatory framework, making it difficult to address emerging issues effectively.

5.2.2 The Cybercrimes Act, 2015

This is a “penal statute intended to deter and discourage privacy and data protection abuses.²⁷⁵ The Cybercrimes Act applies to offences committed within the United Republic of Tanzania,²⁷⁶ including on vessels or aircrafts registered in” Tanzania.²⁷⁷

²⁷² Electronic Transaction Act. No. 13 of 2015. Part III, IV and V

²⁷³ Electronic Transaction Act. No. 13 of 2015. S. 18.

²⁷⁴ Electronic Transaction Act. No. 13 of 2015. S. 14.

²⁷⁵ Cybercrimes Act, 2015. Preamble

²⁷⁶ Cybercrimes Act, 2015. S. 2

The Act criminalizes fraudulent activities committed online *i.e.* identity theft,²⁷⁸ phishing, online scams, electronic forgery,²⁷⁹ unauthorized use of electronic document or records, hacking and other forms of data breaches. Further to that, it protects consumers from cyber harassment, online bullying and threats.²⁸⁰ In addition, it provides legal provisions to prosecute individuals or groups involved in defrauding e-commerce consumers.²⁸¹ It plays a crucial role in protecting e-commerce consumers as the main part in digital economy by addressing various forms of cybercrime and establishing legal mechanism for their prosecution. By deterring and punishing cybercriminal activities, the Act promotes a safer and more secure e-commerce environment, enhancing consumer confidence in online transaction.

5.2.3 The Electronic and Postal Communications Act No.3 of 2010 (EPOCA)

The Act promote consumer protection in electronic transactions. It mandates service providers to uphold consumer rights and provide transparent information about goods, services, pricing, terms, and conditions. a framework for telecommunication sector hence implementing e-government practices in the country.²⁸² Moreover the Act imposes obligations on service providers to implement appropriate security measures to safeguard consumers' personal and financial information.²⁸³ This helps prevent unauthorized access, interception, or manipulation of data during e-

²⁷⁷ Cybercrimes Act, 2015. S. 30(1)(b).

²⁷⁸ Cybercrimes Act, 2015. S. 15(1)

²⁷⁹ Cybercrimes Act, 2015. S. 11

²⁸⁰ Cybercrimes Act, 2015. S. 23(1)

²⁸¹ Cybercrimes Act, 2015. S. 30!)&(2).

²⁸² The Electronic and Postal Communications Act No.3 of 2010. S.

²⁸³ The Electronic and Postal Communications Act No.3 of 2010. S. 98(1)

commerce transactions. On the other hand, EPOCA prohibits unfair trade practices in electronic communications, including deceptive advertising, misleading representations, and unfair contract terms.²⁸⁴ It establishes mechanisms for the resolution of disputes related to electronic communications. ensures that e-commerce consumers have avenues for resolving any conflicts or grievances that may arise during their online transactions. EPOCA regulates the licensing and operation of service providers involved in electronic communications and e-commerce.²⁸⁵ It establishes requirements and standards that service providers must adhere to, ensuring their reliability, trustworthiness, and compliance with consumer protection measures.²⁸⁶ This helps create a more secure and reliable e-commerce environment for consumers.

5.2.4 The Electronic Money Regulations 2015

The Electronic Money Regulations of 2015 is a BOT regulation which is administered by the Bank of Tanzania (BOT). It is the regulation that provides the procedure for granting and refusal of licenses.²⁸⁷ The Bank here also supervises the non-financial institutions together with financial institutions and their agents in order to oversee all their operations.²⁸⁸ These regulations requires service providers to disclose clear and accurate information about their services, fees, terms, and

²⁸⁴ The Electronic and Postal Communications Act No.3 of 2010. S. 60

²⁸⁵ The Electronic and Postal Communications Act No.3 of 2010. Part II

²⁸⁶ Ibid

²⁸⁷ The Electronic Money Regulation, 2015. R. 3 & 4

²⁸⁸ The Electronic Money Regulation, 2015. R. 12

conditions to consumers.²⁸⁹ It further requires electronic money issuers implementing robust security protocols, encryption, and fraud prevention mechanisms to safeguard consumer funds and personal information.²⁹⁰ Also requires providers to have clear and accessible procedures for handling consumer complaints and grievances.²⁹¹ This ensures that consumers have recourse in case of any disputes or issues that may arise during their electronic money transactions.²⁹² Also Providers must meet specific criteria and obtain licenses from the relevant regulatory authority, such as the Bank of Tanzania,²⁹³ and finally the regulations empower regulatory authorities to monitor and enforce compliance with electronic money regulations.²⁹⁴

5.3 Strategy and Policies

Tanzania has implemented various policies and strategies to govern the digital economy and promote its growth. These policies and strategies provide a framework for regulating digital activities, encouraging innovation, and addressing challenges in the digital realm. Here are some of the key policies and strategies governing the digital economy in Tanzania.

5.3.1 Tanzania Digital Economy Strategic Framework 2024 - 2034

The Tanzania Digital Economy Strategic Framework 2024 - 2034 was developed in response to the increasing importance of digital technologies in driving economic

²⁸⁹ The Electronic Money Regulation, 2015. R. 44

²⁹⁰ The Electronic Money Regulation, 2015. R 43

²⁹¹ The Electronic Money Regulation, 2015. R. 45(1)

²⁹² Ibid

²⁹³ The Electronic Money Regulation, 2015. R. 14

²⁹⁴ The Electronic Money Regulation, 2015. R, 46

growth and enhancing service delivery.²⁹⁵ The rationale behind this framework is to create a cohesive strategy that leverages digital transformation to improve public services, boost economic productivity, and enhance consumer engagement. It aims to address the challenges posed by a rapidly changing digital landscape and ensure that all citizens can benefit from digital innovations while protecting their rights and Basic Principles of the Instrument.

The framework is based on several fundamental principles as follows; (1) Inclusivity: ensuring that digital transformation benefits all segments of society, including marginalized and underserved communities, to promote equitable access to digital services.²⁹⁶ (2) Consumer Protection: Prioritizing the protection of consumer rights in digital transactions and ensuring that individuals are safeguarded against fraud and exploitation.²⁹⁷ (3) Data Privacy and Security: Emphasizing the need for robust data protection measures to secure personal information and maintain consumer trust in digital platforms.²⁹⁸ (4) Collaboration and Stakeholder Engagement: Encouraging partnerships between government, private sector, and civil society to foster innovation and address challenges in the digital economy.²⁹⁹

²⁹⁵ Government of Tanzania, Ministry of Information, Communication and Information Technology. (2024). Tanzania Digital Economy Strategic Framework 2024-2034. Retrieved from www.mawasiliano.go.tz/tanzania-digital-economy-framework-2024-2034.pdf Pg. i

²⁹⁶ Government of Tanzania, Ministry of Information, Communication and Information Technology. (2024). Tanzania Digital Economy Strategic Framework 2024-2034. Section 3.4 Pillar 3, Pg. 38/99

²⁹⁷ Government of Tanzania, Ministry of Information, Communication and Information Technology. (2024). Tanzania Digital Economy Strategic Framework 2024-2034. Section 3.2 Pillar 1, Pg. 20/99

²⁹⁸ *ibid*

²⁹⁹ Government of Tanzania, Ministry of Information, Communication and Information Technology. (2024). Tanzania Digital Economy Strategic Framework 2024-2034. Section 3.7 Pillar 6, Pg. 48/99

Overall, the Tanzania Digital Economy Strategic Framework 2024-2034 takes a multifaceted approach to ensuring the protection and empowerment of digital economy consumers through policy, infrastructure, and capacity-building initiatives.

5.3.2 The National ICT Policy 2023

The National ICT Policy 2023 in Tanzania includes provisions aimed at protecting digital market consumers. Below are some key aspects of the policy that contribute to consumer protection in the digital market:

The policy emphasizes the importance of robust regulatory enforcement and continuous monitoring of the digital market to ensure compliance with consumer protection measures.³⁰⁰ It mandates the establishment of dedicated regulatory bodies or the enhancement of existing consumer protection agencies to oversee and enforce digital consumer protection regulations. The policy also emphasizes the importance of digital inclusion, ensuring that all citizens have access to affordable and quality digital services.³⁰¹ Further to that the National ICT Policy acknowledges the significance of data protection and privacy in the digital space.³⁰² It emphasizes the need for robust data protection regulations and the establishment of a legal framework to safeguard personal data. By protecting consumer data from unauthorized access, misuse, or exploitation,³⁰³ the policy helps maintain consumer trust and confidence in the digital market. Next, the National ICT Policy highlights the need for effective grievance redress mechanisms for consumers in the digital

³⁰⁰ The ICT Policy 2023. Chapter 3.7

³⁰¹ The ICT Policy 2023. Chapter 3.10.3

³⁰² The ICT Policy 2023. Chapter 3.2.2

³⁰³ The ICT Policy 2023. Chapter 3.2

market. It encourages the establishment of accessible and efficient mechanisms to resolve consumer complaints and disputes arising from digital transactions. Additionally the policy emphasizes the importance of cybersecurity measures to protect consumers from cyber threats and online fraud.³⁰⁴ Protecting consumers from cybercrimes and promoting secure online environments is an essential aspect of consumer protection in the digital market. By encompassing these consumer protection elements, the National ICT Policy 2023 aims to create a secure and consumer-friendly digital market environment in Tanzania.

5.3.3 The National Records and Archives Management Policy, 2011

The Policy³⁰⁵ provides that public offices shall make sure that all records created or received in the course of government business are captured in record keeping systems with sufficient information (metadata) about the record and its record keeping system, to enable the records to be understood and used for as long as it is needed to transact government business;³⁰⁶ it also requires the government to develop and approve standards, procedures and guidelines for the management of electronic documents and records as well as ensure that electronic records are migrated to new generation of systems whenever there is technological obsolescence.³⁰⁷

5.4 Legal Challenges facing Consumer Protection Framework in Tanzania

Tanzania as a State has made significant steps in consumer protection laws. Over time the state has passed laws, enhance powers of authorities and establishes new

³⁰⁴ The ICT Policy 2023. Chapter 3.3.2

³⁰⁵ The National Records and Archives management Policy, 2011. Part 4.3.

³⁰⁶ Ibid

³⁰⁷ Ibid

sectors for such purpose.³⁰⁸ Moreover compared to the above discussed International and Regional Instrument, it faces several challenges and gaps in consumer protection as discussed below.

First, Tanzania has no specific body mandated to regulate privacy and data governance.³⁰⁹ The existence of separate regulatory bodies for financial services and communications creates legal contradictions and challenges when it comes to addressing digital economy issues. The Primary Regulatory bodies are; the Bank of Tanzania (BOT) as the financial regulator³¹⁰ and the Tanzania Communication Regulatory Authority (TCRA) as the communication regulator.³¹¹ The legal contradiction arise due to the overlapping nature of the digital economy activities that involve both financial services and communication aspects.³¹² For instance, mobile payment systems, digital banking and fintech platforms often involve the use of telecommunication infrastructure and fall within the purview of both the BOT and TCRA. This division of regulatory authority often leads to inconsistency, gaps, and potential conflicts in addressing digital economy issues effectively.³¹³

Secondly, the country lacks comprehensive and specific legislation that addresses consumer protection in the context of e-commerce. Existing consumer protection

³⁰⁸ The Right to Privacy in the United Republic of Tanzania. Stakeholder Report Universal Periodic Review. https://cipesa.org/?wpfb_dl=212 Accessed on 12th April 2024

³⁰⁹ CIPESA. (2022) .Data Governance Regulation in Tanzania. Gaps, Challenges, and Opportunities.. Pg. 12.

³¹⁰ CAP 342, 2006

³¹¹ No. 12 of 2003

³¹² Ibid.

³¹³ Ibid.

laws do not adequately covers the unique challenges and risks associated with digital transactions. Further, there are no existing regulations to provide for legal procedures, manners and circumstances under which data can be disclosed by third party, including law enforcement agencies.³¹⁴ Without these legal protections and procedural safeguards in place, the government has few restriction on how to handle personal data collected through data collected innitiatives such as a SIM Card registration as well as the National ID registration.³¹⁵

Third, protection of data in the digital environment requires advanced technology to track down data breaches and offenders. This requires the law enforcement agencies to have the capacity and the tool to investigate and prosecute data privacy breaches and related cyber crimes.³¹⁶ In Tanzania such capacity is lacking since the cyber crime Unit of the Police force barely has 3 offices in the country. Having few units makes it hard to conduct thorough and timely investigation.³¹⁷

Third, while the number of Tanzanian accessing the internet is rising. There is a concerning disparity between the increasing user base of digital technologies and the level of awareness among users regarding cyber risks. A significant portion of internet users remain unaware of the existence of cyber crime or the importance of safeguarding their data privacy.³¹⁸ Even among those who recognize the necessity of

³¹⁴ CIPESA. (2022). Data Governance Regulation in Tanzania. Op Cit Pg. 12

³¹⁵ CIPESA. (2022). Collaboration on international ICT Policy. Capacity Building and skills development. Ritrieved from https://cipesa.org/?wpfb_dl=212 on 24 Febreary,2014

³¹⁶ CIPESA. (2022). Data Governance Regulation in Tanzania. Op Cit. Pg. 13

³¹⁷ Ibid

³¹⁸ CIPESA. (2022).Collaboration on international ICT Policy. Capacity Building and skills development. Ritrieved from https://cipesa.org/?wpfb_dl=212 visited on 12th April 2024

protecting their privacy, there is a scarcity of knowledge regarding the methods and practices to effectively do so.³¹⁹ On the other hand many victims of personal data breaches do not report to the authorities. Reason being not knowing where to seek remedial measures, fear of being the subject of public ridicule and having little confidence that the relevant authorities would take action against the perpetrators.³²⁰

Fourth, the existing mechanism for consumer redress, such as dispute resolution processes, and tribunals do not adequately serve the purpose and also lacking accessibility. Consumer face challenges in navigating these processes and obtaining timely and satisfactory resolution to their complaint. In Tanzania there are specific and general consumer remedies set out in various legislations which makes it difficult for the consumers to pursue their rights and businesses to meet compliance costs.³²¹ It is costly for a consumer to recover a loss or damage through action in a court of competent jurisdiction as it is provided for under Part VI and VII of the Fair Competition Act.³²²

5.5 Regulatory framework

In Tanzania, the potential of the digital economy to drive economic growth, innovation, and social development has been recognized, leading to the establishment of institutional framework. This Part provides an overview of the institutional framework that governs the digital economy in Tanzania, highlighting key

³¹⁹ Supra Note 336

³²⁰ CIPESA. (2022). Data Governance Regulation in Tanzania. Op Cit. Pg. 14

³²¹ Kilenga P, J. (2023). Consumer Protection in Tanzania. Research Gate Publication Pg. 11

³²² Ibid

institutions and their roles in fostering a conducive environment for digital innovation and entrepreneurship.

5.5.1 Tanzania Computer Emergence Response Team TZ-CERT

TZ-CERT (Tanzania Computer Emergency Response Team) is a specialized institution responsible for protecting the digital economy in Tanzania from online threats³²³ and ensuring the security and resilience of information and communication technology (ICT) infrastructure,³²⁴ it plays a crucial role in safeguarding the digital ecosystem in the country. TZ-CERT currently provides the following services to its constituencies and general public. First; alert, warning and announcements,³²⁵ the organ is constantly monitoring cyber security threat and vulnerabilities and can advise both the constituency member and the general public.³²⁶ Second: incident response, the organ work with constituency organization to respond to all cyber security threat in their respective network also provide step by step assistance to organization that face cyber security attacks.³²⁷ Third, the organ is working on disseminating the cyber security information to the community. This includes promoting cyber security best practice to the technology users. Fourth, to provide organization with assistance in order to discover potentials vulnerabilities to their

³²³ The Electronic and Postal Communications Act No.3 of 2010. S. 124

³²⁴ TZ-CERT About Us. Retrieved <https://www.tzcert.go.tz/about-us/tz-cert-profile/> accessed on 23rd Feruary 2024

³²⁵ TZ-CERT. Vulnerabilities. Retrieved from <https://www.tzcert.go.tz/vulnerabilities> accessed on 3rd May 2024

³²⁶ TZ-CERT. Our services. Retrieved from <https://www.tzcert.go.tz/services/> accessed on 3rd May 2024

³²⁷ Ibid

systems and Network Infrastructure.³²⁸ And finally digital forensic investigations which covers both computer and network forensic investigation on the reported incidents for the purpose of evidence collection.

5.5.2 Tanzania Data Protection Commission

The Tanzania Data Protection Commission (TDPC) as an offshoot of Tanzania Communication Regulatory Authority plays a crucial role in governing the digital economy by safeguarding individuals' privacy rights and ensuring the responsible handling of personal data.³²⁹ As the regulatory body responsible for data protection in Tanzania, the TDPC is tasked with enforcing data protection laws, promoting best practices, and protecting the rights of individuals in the digital sphere.³³⁰ among others TDPC has the following duties; it examines complains from individuals in relation to potential infringements of data protection law,³³¹ conduct inquiries and investigations³³² and take enforcement³³³ actions where necessary,³³⁴ promotes awareness among members of the public to have their personal information protected under data protection law;³³⁵ drive improved awareness and compliance with data protection legislation by data controller and processors legislation through the

³²⁸ TZ-CERT. Our services. Retrieved from <https://www.tzcert.go.tz/services/> accessed on 3rd May 2024

³²⁹ The Personal Data Protection Act, CAP 44, 2022. S. 4

³³⁰ Personal data protection commission. Establishment. Retrieved from <https://www.pdpc.go.tz/en/about-pdpc/establishment/> accessed on 3rd May 2024

³³¹ Data Protection Commission. What we do. Retrieved from <https://www.dataprotection.ie/en/who-we-are/what-we-do> accessed on on 3rd May 2024

³³² The Personal Data Protection Act, CAP 44, 2022. S. 39

³³³ The Personal Data Protection Act, CAP 44, 2022. S. 40

³³⁴ Ibid

³³⁵ The Personal Data Protection Act, CAP 44, 2022. Part V

publication of high quality guidance and proactive engagement; Moreover It shares information, best practices, and experiences to enhance the effectiveness of data protection regulation.³³⁶

5.5.3 Tanzania Communications Regulatory Authority

The Tanzania Communications Regulatory Authority (TCRA)³³⁷ plays a crucial role in governing the digital economy in Tanzania. As the primary regulatory body for electronic communications, the TCRA is responsible for ensuring compliance with relevant laws, promoting fair competition, protecting consumer rights, and fostering the growth of the digital sector.³³⁸ TCRA is responsible for issuing licenses to telecommunications operators, internet service providers (ISPs), content providers, and other entities involved in the digital economy.³³⁹ It also establishes rules and regulations to protect consumers from unfair practices, misleading advertisements, and substandard service quality. In addition to that TCRA handles consumer complaints, conducts investigations, and takes appropriate actions against service providers who violate consumer rights.³⁴⁰ Nonetheless, TCRA actively engages with various stakeholders, such as industry players, consumer associations, civil society organizations, and government agencies in regulating communication and data protection.³⁴¹

³³⁶ The Personal Data Protection Act, CAP 44, 2022. S. 7(g)

³³⁷ The Tanzania Communications Regulatory Authority Act 2003. S. 4

³³⁸ Tanzania Communications Regulatory Authority Act 2003. S. 5

³³⁹ The Electronic and Postal Communication Act, CAP 306 R.E. 2022 (S. 4 to S. 26)

³⁴⁰ The Tanzania Communications Regulatory Authority Act 2003 (S. 40 to S. 44)

³⁴¹ The Tanzania Communications Regulatory Authority Act 2003. S. 22

5.5.4 Fair Competition commission

The Tanzania Fair Competition Commission (FCC)³⁴² plays a crucial role in governing the digital economy by promoting fair competition, preventing anti-competitive practices,³⁴³ and protecting consumer interests.³⁴⁴ The FCC operates within the legal framework provided by the Fair Competition Act. This act prohibits anti-competitive agreements,³⁴⁵ abuse of dominant market positions, and mergers or acquisitions that may substantially lessen competition.³⁴⁶ Next to that, the FCC investigate complaints, conduct market studies,³⁴⁷ and take appropriate actions against entities engaged in anti-competitive practices.³⁴⁸ Also as well the FCC is responsible for reviewing mergers and acquisitions in the digital sector to ensure they do not harm competition or consumer welfare.³⁴⁹ Further to that, the FCC collaborates with other regulatory authorities,³⁵⁰ industry associations, and consumer organizations to promote fair competition and consumer protection in the digital economy. Moreover the FCC conducts capacity-building programs and awareness campaigns to enhance understanding of competition law and its application in the

³⁴² The Fair Competition Act No. 8 of 2003. S. 62(1)

³⁴³ Fair Competition Commission – For Fair Play in the Economy. Mandatory Functions. Retrieved on 25th February 2024 from <https://www.fcc.go.tz/functions/>

³⁴⁴ Martha Kisyombe. (July 2012). Paper for presentation at UNCTAD ad-hoc expert group meeting on the interface between competition policy and consumer welfare Retrieved from https://unctad.org/system/files/non-official-document/ciclp2012_EMCP_S3_Kisyombe_en.pdf#:~:text=The%20Fair%20Competition%20Commission%20is%20an%20independent%20government,Act%20contains%20both%20competition%20and%20consumer%20protection%20provisions. Pg. 9 accessed on on 23rd February 2024

³⁴⁵ The Fair Competitions Act No. 8 of 2003. S. 8&9

³⁴⁶ The Fair Competition Act. No. 8 of 2003. S.

³⁴⁷ The Merchandise Marks Act CAP 85. S. 2B, read together with R. 3 of the Merchandise Marks Regulations 2008

³⁴⁸ The Fair Competitions Act, 2003. Part III

³⁴⁹ The Fair Competitions Act No. 8 of 2003. S. 11

³⁵⁰ The Merchandise Marks Regulations 2008. R. 4(1)

digital economy.³⁵¹ Finally, FCC collaborates with counterparts from other countries and engages in knowledge-sharing, capacity-building, and enforcement cooperation.

Its important to note that, all these institutions works closely with the Tanzania Police Force. Tanzania Police Force is the State body mandated with the duty to protects citizens and their properties.³⁵² Itself has a specialised cybercrime force Unit that deals solely with the computer related crimes.³⁵³

5.4 Comperative Analysis Between Tanzania, South Africa and Kenya

South Africa, Kenya, and Tanzania are three countries in Africa with emerging e-commerce markets. While both countries have implemented consumer protection frameworks to regulate online transactions and protect consumers,³⁵⁴ there are still significance differences that requires comparison discussion. The differences in e-commerce consumer protection framework can be categorized in; scope of legislation, regulatory bodies, consumer redress and enforcement mechanism. While both South Africa and Kenya have established specific regulatory bodies, such as the National Consumer Commission (NCC)³⁵⁵ and the Consumer Goods and Services Ombud (CGSO), Kenya Consumer Protection Advisory Committee (CPAC)³⁵⁶ respectively, to oversee consumer protection in e-Commerce, Tanzania on the other hand, has a general regulatory body, the Fair Competition Commission (FCC), which

³⁵¹ The Fair Competition Act, 2003. S. 65(2)(c)&(d)

³⁵² CIPESA, (2022) Data Governance Regulation in Tanzania. Op Cit. Pg. 11

³⁵³ Ibid

³⁵⁴ Ibid

³⁵⁵ The South African Consumer Protection Act. No. 68 of 2008. S. 85

³⁵⁶ Ibid

among others also handles consumer protection matters.³⁵⁷ This generality has effects on the performance of the regulatory body in consumer protection since it has plenty other responsibilities to take care of. On scope of Legislation, South Africa has a relatively more developed and comprehensive consumer protection framework, namely the Consumer Protection Act (CPA). The CPA covers various aspects of consumer protection, including unfair marketing practices, product safety, and unfair contract terms (as discussed above in preceding chapter), while also Kenya's CPA covers various aspects of consumer protection, including unfair trade practices, product safety, and consumer rights enforcement.³⁵⁸ Tanzania on the other hand, consumer protection framework is still evolving, and it primarily focuses on anti-competitive practices and fair trade.³⁵⁹ On the aspect of online dispute resolution, both South Africa and Kenya have introduced online dispute resolution mechanisms to facilitate the resolution of e-commerce disputes.³⁶⁰ These mechanisms provide an alternative to traditional legal procedures and aim to expedite the resolution process.

Tanzania, however, does not currently have specific provisions for online dispute resolution. In Tanzania Consumers can file complaints directly with the FCC or the Tanzania Communications Regulatory Authority (TCRA), or The Tanzania Consumer Advocacy Society (TCAS). Both these Regulatory bodies offer ADR services like mediation and conciliation to help resolve consumer disputes. Nonetheless, these methods require time and money that some consumers may not

³⁵⁷ Ibid

³⁵⁸ ibid

³⁵⁹ Ibid

³⁶⁰ Anthony Mzurikwao. (2018). Influence of Political,. Op Cit. Pg. 84.

have, and consumers quite often choose to ignore their complaints. Also lack of awareness of these methods and the fear of disadvantages when trying to resolve disputes with larger, more established businesses or service providers. Therefore one can say that comparably Tanzania needs to make some more efforts and steps by coming up with proper legislations to govern online transactions, cross border agreements, digital transactions disputes and related digital transactions issues.

5.7 Conclusion

This Chapter has analysed critically the steps taken by the government in consumer protection in the country. Though Tanzania has taken significant steps to establish consumer protection laws and regulations that address the unique challenges posed by online transactions. While the framework is still evolving, it primarily focuses on anti-competitive practices and fair trade. In addition, the existing legislations have various legal gaps in online contracts, dispute settlements, e-taxation, cross border transactions and interoperability. The findings entail as the e-commerce landscape continues to evolve, it is imperative for Tanzania to remain proactive in updating and adapting its legal and regulatory framework to address emerging challenges and protect the rights of consumers.

CHAPTER SIX

SUMMARY OF FINDINGS, CONCLUSION AND RECOMMENDATIONS

6.0 Summary of findings

The principle purpose of this study is to point out the legal and institutional gaps in online consumer protection framework in Tanzania. The analysis was done by examining the existing legal, policies, strategies and regulatory mechanisms in place to safeguard consumers in the context of e-commerce and in comparison to International and Regional convention. In order to achieve the intended objectives the following questions guided the research.

- i. What are the existing legal gaps in the laws regulating consumer protection in Tanzania's digital economy ?
- ii. What is the experience of other jurisdictions regarding Digital Economy and consumer protection?
- iii. What are the international legal instruments and best practices that can provide valuable insights and experience in the field?
- iv. What regulatory framework can be proposed to effectively promote innovation while simultaneously enhancing consumer protection?

In order to assess the adequacy of legal and regulatory framework governing digital market consumer protection in the country, the international and Regional Instruments were employed in the analysis. In addition the discussion invited the experience of other jurisdictions in order to determine their legal position in addressing the same issue. The experience of Kenya, and South Africa were very

useful in providing an overview concerning online consumer protection. However, in these countries the serious challenge remains to be lack of digital literacy and enforcement challenges since enforcing consumer protection regulations in the rapidly evolving digital landscape can be resource-intensive and complex for regulatory authorities.

6.1 The study

The study has answered extensively all four questions that were raised at the beginning of the study. The findings of the study have revealed that, the existing legislations in the country are inadequate and do not offer enough protection to the online consumers. There are several legal gaps in the Electronic Transaction Act, 2015, the fair competition Act, 2003, Electronic and Postal Communication Act, 2010, the Electronic Money Regulations, 2015 etc. All these legislations have not digested extensively legal issues brought digital market economy. Issues such as specific legislation that addresses consumer protection in the context of e-commerce, dispute settlement (ODR), Technological prowess to investigate and prosecute data privacy breaches and related cyber crimes³⁶¹, Uneven Access to Digital Services.

6.2 Conclusion

In conclusion, this dissertation has shed light on the consumer protection framework in Tanzania, its strengths, weaknesses, and areas for improvement. Enhancing consumer protection requires a collective effort from regulators, businesses, civil

³⁶¹ Supra Note 339

society organizations, and consumers themselves. By implementing the recommended measures and continuously evaluating and adapting the framework, Tanzania can foster a robust and responsive consumer protection environment, ensuring that consumers are empowered, informed, and protected in the marketplace. Ultimately, a strong consumer protection framework contributes to a fair and sustainable economy, benefiting both consumers and businesses alike.

6.4 Recommendation

In light of the foregoing and with the goal of supporting e-commerce consumer rights and protection the following are recommended;

Tanzania should establish Online Dispute Settlement mechanism with simple procedures and fairness with no charges to encourage consumers to file complaints without incurring extra costs. These mechanisms provide an alternative to traditional legal procedures and aim to expedite the resolution process. This can include setting up dedicated e-commerce dispute resolution bodies or utilizing existing consumer protection agencies. Furthermore, Tanzania should establish comprehensive legislations and Regulations specifically tailored to e-commerce consumer protection to cover areas such as online transactions, dispute resolutions and consumer rights. On the other hand, the Government should Strengthen enforcement mechanism to ensure compliance with e-commerce consumer protection laws and regulations. This involve increasing resources to consumer protection agencies and conduct regular audits

Also, regular evaluation on effectiveness of consumer protection measures and adopt them to evolving e-commerce trends and challenges. To stay updated on international developments in e-commerce consumer protections. And lastly, is to promote consumer education and awareness programs to educate Tanzanian consumers about their rights and responsibilities when engaging in e-commerce transactions. This can continue to be done through public campaigns, workshops and online resources. Efforts to increase consumer awareness should be significantly expanded in rural areas, as consumers there require greater parity with urban areas. Specific initiatives targeting elderly populations are needed to educate them on the use of digital marketplaces.

BIBLIOGRAPHY

- Adam, J & Kamuzora, F., *Research Methods for Business and Social Studies*. Tanzania, Dar es Salamm, Mzumbe Book Project, 2008. At pg.115.
- Atikah, I. “Consumer Protection and Fintech Companies in Indonesia: Innovations and Challenges of the Financial Services Authority.” *Jurnal Hukum Dan Peradilan* 9, no. 1 (2020): 132. <https://doi.org/10.25216/jhp.9.1.2020.132-153>.
- Banga, K, and D W te Velde. “Covid-19 and Disruption of the Digital Economy; Evidence from Low and Middle-Income Countries.” *Digital ...*, 2020. https://pathwayscommission.bsg.ox.ac.uk/sites/default/files/2021-01/covid-19_and_disruption_of_the_digital_economy_28jan21.pdf.
- Best, L., and M Struwig. “Online Business Practices to Enable Consumer Protection in the African Context.” *International Journal of Economics, Business and ...* 4, no. 10 (2020): 118–32. [https:// www. ijebmr. com/ uploads/ pdf/ archivepdf/ 2020/IJEBMR_624.pdf](https://www.ijebmr.com/uploads/pdf/archivepdf/2020/IJEBMR_624.pdf).
- BoT, *Electronic Banking Annual Report*, Bank of Tanzania, 2019.
- Brown, P., *A reviews of the Literature reviews on case study research design*, 1 (1) *Open Journal System*, 2008, at Pg. 5-25.
- Carvalho, M., “European Consumer and Market Law” 9, no. June (2020): 89–92.
- Cash M., & Scholar R., *Electronic Commerce and Tax Base Erosion*, European Parliament, 3 (1) “Directorate General for Research” Luxembourg 1999.
- Christopher, J., *Why Digital economy Giants Exit Tanzanian Market?* Retrieved from <[http:// https://www.google.com/search?q=why+digital+economy+](http://https://www.google.com/search?q=why+digital+economy+)

giants+ exit+ tanzanian+ market &rlz= 1C1JZAP _enTZ938TZ 938&oq
=why+digital economy+ giants+ exit+ tanzanian+ market &aqs=
chrome. 69i57j33i160.20385j0j15&sourceid=chrome&ie=UTF-8>

Chuwa, H., Analysis of the Law Governing Digital economy in Tanzania, LLM
Dissertation, OUT, 2014.

CIPESA, ICT in Governance in Tanzania – Policies and Practice, CIPESA ICT
Research Series No. 07/15 October, 2015.

Dahlman, C., Sam; M., and Martin W., “Harnessing the Digital Economy for
Developing Countries.” OECD Development Centre Working Papers,
no. 334 (2016): 1–77. [https://www.oecd-
ilibrary.org/docserver/4adffb24-
en.pdf?expires=1674044903&id=id&accname=guest&checksum=1249
F8F04498C0B269E3044B0436DBD8](https://www.oecd-ilibrary.org/docserver/4adffb24-en.pdf?expires=1674044903&id=id&accname=guest&checksum=1249F8F04498C0B269E3044B0436DBD8).

Dynamics, Development. “Why Business Schools In Tanzania Should” 30, no. 1
(2020): 37–68.

Emmanuel C. L., and Kwangho J., ‘E-Government Transformation in Tanzania:
Status, Opportunities, and Challenges,’ The Korean Journal of Policy
Studies, Vol. 30, No. 1 (2015), pp. 147-184.

Garz, S., Xavier G., Dean K., Rafe M., Caitlin S., and Jonathan Z., “Consumer
Protection for Financial Inclusion in Low- And Middle-Income
Countries: Bridging Regulator and Academic Perspectives.” Annual
Review of Financial Economics 13 (2021): 219–46. [https:// doi.
org/10.1146/annurev-financial-071020-012008](https://doi.org/10.1146/annurev-financial-071020-012008).

- Gwakisa A. K., The Legal And Regulatory Frameworks And Infrastructures For E-Government Initiatives In Tanzania: A Critical Review, as available at http://www.saarchivist.co.za/images/documents/Past%20events/2012%20Conference%20papers/Gwakisa%20Kamatula_0.pdf accessed on 27th May, 2022. <https://aisel.aisnet.org/whiceb2019/42>.
- Ibrahim, Pei, Yang, and Chang, J., "Challenges of Cross Border Digital economy in Tanzania: A Case Study of Tanzania in Comparison with CHINA" (2019). WHICEB 2019 Proceedings. 42.
- Jim Y., Adoption of Transactional Level e-Government Initiatives in Tanzania, 2013, as available at http://www.clknet.or.tz/wp-content/uploads/2014/02/FV_Adoption-of-Transactional-Level-e-Government-Initiatvies-in-Tanzania-With-interview.pdf accessed on 27, 2022.
- Kato, C., "Legal Framework Challenges to E-Banking in Tanzania, 3 (2) Research Reviews, 2019 at Pg.101-110.
- Keck, M., Seharish G., Ahmed D., and Jeremiah G., "The Role of Consumer Protection in the Digital Economy," 2021.
- Kemp, S., Digital 2020: Tanzania, Available at: <https://datareportal.com/reports/digital-2020-tanzania>.
- Keneth, et al, Digital economy Trend in Developing countries: A case Study in Tanzania, International Journal of Computer Application. (2015).
- Lemma, A., Max M., and Laura N., "The AfCFTA : Unlocking the Potential of the Digital Economy in Africa," 2022.
- Lupilya, E & Jung, F., E-Government Strategic Plan Implementation in Tanzania, 30 (2) The Korean Journal of Policy Studies, 2015 at Pg. 147-175.

- Mambi, A., *ICT Law Book; A Source Book for Information & Communication Technologies and Cyber Law*, Mkuki na NYota, Tanzania, 2010.
- Maruma, Z., “Legal and Institutional Challenge Facing Digital economy in Tanzania. LLM IT & T of OUT, 2013.
- Masamila, B., “State of Mobile Banking in Tanzania and Security Issues.” *International Journal of Network Security & Its Applications* 6, no. 4 (2014): 53–64. <https://doi.org/10.5121/ijnsa.2014.6405>.
- Mollel E., “The Legal Basis of Electronic Banking” LLM Dissertation University of Dar es salaam, Dar es salaam 2016.
- Mtaita, G., Nyanjige M., and Amembah A L A., “Assessment of the Practice of Digital Disbursement Financial System in Managing Student’s Loans among Higher Learning Institutions in Northern Zone Tanzania.” *Asian Journal of Humanities and Social Studies* 9, no. 4 (2021): 170–80. <https://doi.org/10.24203/ajhss.v9i4.6746>.
- Mugume, R., and Enock W.N., “Post-COVID-19 Recovery for African Economies: Lessons for Digital Financial Inclusion from Kenya and Uganda.” *African Development Review* 34, no. S1 (2022): S161–76. <https://doi.org/10.1111/1467-8268.12652>.
- Mutagahywa, B., *Connectivity and Digital economy*, Economic and Social Research Foundation (ESRF), UDSM, 2000.
- Mwakatumbula, H., “Consumer Protection in the Telecommunication Markets in the Post Liberalization Era-the Case of Tanzania,” no. March (2017).

- Mwamsoda, U., Ojwag, E., & Pastory, D., Examining the Consumer Protection and Comprehensiveness in Digital economy in Tanzania, 4 (1) Business Educational Journal, 2020 at Pg.1-12.
- Njau, L., Challenges of Consumer Protection in Digital economy in Tanzania, 7 (6) Journal of Legal Studies and Research, 2021, at Pg.110-118.
- Nkohkwo, Q., & Islam, S., Challenges to the Successful Implementation of E-government Initiatives in Sub- Saharan Africa, 11 (2) Electronic Journal of e-Government, 2013 at Pg.253-267.
- Oreku, G., A View Point of Tanzania Digital economy and Implementation barriers, 10 (1) ComSIS, 2013 at Pg. 264-281.
- Quinta N N., and Sirajul I. M., ‘Challenges to the Successful Implementation of e-Government Initiatives in Sub-Saharan Africa: A Literature Review,’ Electronic Journal of e-Government, Volume 11, Issue 2, 2013.
- Rafe M., and Philip R., “Competition in Mobile Financial Services: Lessons from Kenya and Tanzania.” The African Journal of Information and Communication (AJIC), no. 17 (2016): 39–59. <https://doi.org/10.23962/10539/21629>.
- Reed, C., Internet Law; Text and Materials (2nd) Cambridge University Press, U.S, 2004.
- Shigella E.E., “the Effect of Digital economy on Tax Laws in Tanzania (the case study of income tax and vat laws administered by the Tanzania Revenue Authority” Open University of Tanzania 2013.
- Turban, E., King, D., & Lee, K., Electronic Commerce; A Managerial and Social Networking Perspectives, Person Education, U.S, 2008.

Tygar, Atomicity in electronic commerce, Chapter 33. In *Internet Besieged*, P. Denning, D. Denning (eds.). ACM Press and Addison Wesley, USA, 1997, pp. 389– 405.

UN, *Cyber Laws and Regulations for Enhancing Digital economy*, United Nations Conference on Trade and Development; January 14, 2015.