IMPACT OF TECHNOLOGICAL ADVANCEMENTS ON TRADE IN RELATION TO THE LAW IN KENYA

BY

GERALD MBURU NG'ANG'A

AD101357

A DISSERTATION SUBMITTED TO THE RIARA UNIVERSITY IN PARTIAL FULFILMENTT OF THE REQUIREMENTS FOR THE DEGREE OF BACHELOR OF LAWS (LLB)

APRIL 2021

NAIROBI, KENYA

DECLARATION

I, GERALD MBURU NG'ANG'A declare that "IMPACT OF TECHNOLOGICAL ADVANCEMENTS ON TRADE IN RELATION TO THE LAW IN KENYA" is my own work, that it has not been submitted for any degree or examination in any other university or institution, and that all the sources I have used or quoted have been indicated and acknowledged by complete references.

Signature: _____

Name: **GERALD MBURU NG'ANG'A**

Date: **APRIL 2021**

ABSTRACT

Technology refers to the application of scientific knowledge for practical purposes, especially in the industry field. Over the years, there has been a surge in the technological field with the invention of new machinery and equipment. This development has in turn brought about adverse effects to the lifestyle of man, with most activities meant to be carried out by man being handled by machines.

It has to be noted however that with this kind of improvement on man's standard and ways of living, there has also been a tremendous impact on the law at large. With new mechanisms being put in place to improve the livelihood of man, there has been a need also to come up with laws and policies that would ensure such advantages are not violated and are in the scope of the general public interest. For instance, policies and guidelines would be a good starting point to ensuring that such advancements are legal.

The Internet is the major advancement that has changed the ways of man overtime. Since the invention of the first computers to the introduction of mobile phones, there has been a major boost in the performance of man especially in the work related field. Most programs are being run by the use of software and don't necessarily need the physical presence of an individual in a given location. A good example would be during the Covid 19 breakout, most activities have been left to the internet to carry out such as learning, trade, religious activities.

This has in turn called for the law to step up and put in place mechanisms that would ensure such activities are in check and don't pose a threat to the well-being of individuals. This paper would attempt to address issues arising from such developments on trade and how the law has been affected. It would also try to establish possible means through which technology can be further improved to best suit the needs of man and the possible resolution to man's problems through the comparison of different mechanisms put in place in different countries.

LIST OF ABBREVIATIONS

CEDAW	Convention on the Elimination of All Forms of Discrimination against Women
CESCR	Committee on Economic, Social and Cultural Rights
ICCPR	International Covenant on Civil and Political Rights
ICESCR	International Covenant on Economic, Social and Cultural Rights
UDHR	Universal Declaration on Human Rights UN United Nations

TABLE OF CASES

TABLE OF LEGAL INSTRUMENTS

Constitution of Kenya, 2010
Chapter 411 A laws of Kenya

Information Technology Act No 21 of 2000, India, Section 3

Contents

1.1. INTRODUCTION

Technology refers to the use of improved machinery by man to carry out assignments with the aim of achieving better results compared to if such an activity was to be carried out manually. Some of the common machinery that are being used by man in performing a myriad of tasks include the use of the internet. The internet was built mainly to enhance communication between individuals.[1] Overtime it has been developed to enhance trade. Many users have adapted to the use of the internet, they use it to conduct transaction such as advertisement of products, selling and buying of products.[2] In the overall context, traditional means of carrying out activities are being archived with practices such as barter trade, which involved the exchange of goods and service has now changed due to the development of technology. In recent times, the technology has been used to achieve economic objectives of providing goods and services to consumers at a more efficient rate. [3]It has created a platform that ensures that goods reach the customers despite of wherever they are or any type of goods that they may require.[4] States have decided to encourage the use of the internet to develop e-marketting as it is also a source of revenue.[5] A wide variety of e-commerce is conducted via the internet this include, money transfer, online marketing, data exchange, online transaction and any other type of business.[6]

---

[1] Cheeseman Henry, (2001), 'Business Law: Ethical, International and E-commerce Environment', 4th Edition, Prentice-Hall Publishers, USA.

[2] Marcum Catherine et al, (2011),'Doing Time for Cybercrime: An Examination of the Correlates of sentence Length in the United States "International Journal of Cyber Criminology, Vol 5 Issue 2 July - December 2011,Georgia

[3] Avtar Singh, (2006).Principle of Mercantile Law, 8th Edition, Eastern Book Company, India.

[4] OECD, (1998) Report on E-commerce p 194. Dismantling the Barrier to Global Electronic Commerce, Finland.19-27 November 1997-Confernece Report, OECD Digital Economy Papers, 38OECD Publishing Report. http://dx.do.org/< accessed on 25th October 2018.
OECD is an international organization whose main aim is to oversee economic development.

[5] C.M.Abhilash, (2002), "E-Commerce Law in Developing Countries: An Indian Perspective", 11(3), Journal of Information and Communication Technology Law, India.

[6] Ibid 4

1.2. BACKGROUND OF THE STUDY

The internet was introduced in Kenya in 1990 by the NGOs.[7] Internet connection was available as from 1995 October courtesy of the African Regional Center for Computing. At this time, the internet was costly and the connection was low.[8] Kenya had to use satellite to boost the connection which proved to be expensive. The internet connection was boasted in 2012 by the submarine cable internet. Since then the internet has grown rapidly due to the increase in the number of user.[9] This development enhanced the advancement in technology which brought forth new opportunities that individuals have opted to exploit. The Kenya Information and Communication Act[10] defines electronic as relating to technology .

In today's world, the use of technology has become the norm of carrying out business. One does not need to own the latest technology to carry out business; it can be conducted via the mobile. Kenya has an estimation of 39.1 million subscribers who use it for mobile transaction and transfer of money.[11] Many individuals have invested more in the technological realm thus developing the economy of the country. With the developing technology, businesses have been granted the opportunity to spread their business globally with less investment, learning can be achieved globally by the use of technology, this resulting into the world being reduced into a technological global village. For example Kenya has a population of 48.46 million individuals and thus the development of the country's economy is crucial.[12] Due to the high population within the country there are inadequate employment, more individual have opted to invest more in e-commerce to create more revenue. The World Health Organization on November 1998 defined e-commerce as the production, distribution, marketing and sale of goods and services through electronic means.

This has boosted the economy of the country generally. The Survey conducted by MasterCard[13] on online shopping reveals that 75% of the individual who shop online are satisfied by the services

[7] Michel M. Murungi, (2011),'Cyber law in Kenya', Kluwer Law International 2011, Kenya.
[8] Enrico Calandro et al, (2012), "Internet Going Mobile: Internet Access and Usage in 11 African Countries," Journal of Research ICT Africa, 2012, Sub Saharan.
[9] The ICT Board connected Kenya 2017 master plan
[10] Chapter 411 A laws of Kenya
[11] McCrohan Kevin, (2003).'Facing the threats to Electronic Commerce', 18(2), Journal of Business & Industrial Marketing, George Mason University.
[12] CCK website, quarterly sector statistics report second quarter of the financial year 2014/15(June-June 2015. http://moseskemibaro.com/2014/07/28/key-highlights-from-the-communication-authority-of-kenya-q3-sector-statistics-report <accessed on 26th October 2018
[13] The survey was conducted on October 7 2016. MasterCard is an international company that is incorporated in the United States of America in 2006. It offers financial services, through debit and credit cards.

provided. They have justified online shopping is convenient and easy. Online shopping allows the consumers to obtain goods that they would otherwise not be obtained since most of the goods are universal. It can be said that electronic commerce has formed part of the daily lives of individuals. We cannot overlook the fact that the more that the technology has developed the more the users. We cannot deny that there are benefits that have accrued to the state's economy but it should not be assumed that there are no adverse challenges that the merchants face.

This chapter is focused on understanding the impacts of technological advancements on trade in relation to the law. It helps in understanding the adverse effects that law has been subjected to. It provides an understanding how different sectors have tried to cope up with the challenges arising out of such practice. There is also need to consider the measures that have been placed by the government to ensure that such developments are beneficial and contribute to the growth of individuals and the economy at large.

1.3. LITERATURE REVIEW

Technology is the use of improved and approved scientific mechanisms in the carrying out of businesses. With the development of technology, there are more cases of cybercrime, cyberbullying, theft, environmental pollution, moral degradation.[14] Several authors have written more concerning the subject of the research. In this thesis we look at the approach of different authors towards the research question. Some of their opinions may be used as preposition in this research

One author, Kshetri[15], elaborates on some of the issues that need to be considered when dealing with e-commerce. Cybercrime has developed due to the development of technology and e-commerce. E-commerce has taken over the human life. It being part of the human life has attracted more cybercriminal who choose to attack such sites to obtained profits. He elaborates that individuals have depended so much on technology, specifically e-commerce.[16] This has caused an

[14] Chouhan Raksha, (2014), 'Cybercrimes: Evolution, Detection and Future Challenges' The IUP Journal of Information Technology, Hyderabad.
[15] Kshetri N, (2010) 'Global Cybercrime Industry, Economic, Institutional and Strategic Perspectives', second Edition, Springer, United State of America.
[16] Camqc Nicholas (2008), 'Emerging Trends in Cyber Crime, 13th Annual Conference - New Technologies in Crime and Prosecution: Challenges and Opportunities', International Association of Prosecutors, Singapore.

overdependence on such thus becoming vulnerable. Most merchants have fallen victims to such people.[17] One of the ways of dealing with cybercrime is the use of digital signatures which is contained in Section 3 of the IT legislation of India (2008)[18] .It is used to authenticate the electronic transaction. In addition, there is need to give it a digital signature certificate so as to validate it. He goes ahead to discuss on issues relating to e-governance. He stipulates that e-governance majorly deals with the issues of electronic governance and the legal regime dealing with e-commerce. He provides that there is need for legal recognition of e-commerce records that can help in achieving justice. The aspect of civil liability is brought forth in this book. He claims that data theft can be done by the employees, who are part of the organization. Company loose more profit to their employees who have decided to conduct themselves in a manner that is a hindrance to the growth of such company. He opines on how some of the merchants have opted not to refer cases to the law enforcement agencies the moment they fall victims to cybercriminals. This has impeded the growth of e-commerce. They are afraid of losing the trust of their customers or even loose them.[19]

Gottschalk[20] engages the aspects of price manipulation and counterfeit products. First price manipulation entails the alteration of prices of goods that have already been advertised. This has become an issue that needs to be dealt with seriously as merchants loose more profits to such. He discusses the fact the cybercriminal is able to access the website of e-merchants and alter the prices. The other issues considered here are the sale of counterfeit goods. The original good may be expensive thus affordable to only a few consumers. He stipulates that cybercriminal use this loophole to create other counterfeit good that they sell at a cheaper price to the unknowing consumers.[21] The manufacturers of such business are more discouraged as they won't be earning any profit from their own work.

With regard to ensuring the merchants deal effectively with cybercrime, Maskowitz[22] elaborates on the measures that have been taken by the merchants in order to protect their own business, while

[17] Ramachnadran Ganesan et al (2010), a novel digital envelope approach for a secure e- commerce channel, International Journal of Network Security, Odisha.
[18] Information Technology Act No 21 of 2000 , India , Section 3
[19] Geeta Virju, (2011), online identity theft-an Indian perspective, 18(3), Journal of Financial Crime, Emerald Group Publishing Ltd. India.
[20] Gottschalk Petter, (2013).Policing cybercrime. First Edition, Ventus publishing Aps, Denmark.
[21] Holt Thomas et al, (2010)," Examining the Social Networks of Malware Writers and Hackers", 6(1), International Journal of Cyber Criminology, Michigan State University.
[22] Maskowitz Sanford, (2017)' Cybercrime and Business: Strategies for Global Corporate Security', First Edition, Butterworth-Heinemann, United States Of America.

making recommendation on certain measures that have been placed. He recounts the various measure placed by the United States of America in order to deal with cybercrime. His wok estimated that the measures taken by the merchants are not sufficient to curb cybercrime. They are insufficient based on the fact that technology changes each time and thus cybercrime develops too in the process. The measures prove to be outdated. He also discusses some of the measures taken by the government in order to ensure that e-business is protected. His work is crucial to this research; it touches on one of the important facets that will ensure the protection of a business. It enables one to analyze and give recommendation on how to deal with such issues

1.4. STATEMENT OF THE PROBLEM

The rapid growth of technology has developed the online marketing industry which has created an extensive e- commerce market across the world.[23] One may transact from anywhere in the part of the world and still receive the desired goods. The mode of payment preferred has been online payment.[24] E-commerce has developed the economy of the state.[25] The development is not rapid since there are other issues that deter it from achieving it potential.[26] One major objective in Kenya Vision 2030[27] is to ensure that the economy of Kenya develops. E-commerce promotes the economic development but this cannot be achieved yet.

One of the major issues that impede the development of e-commerce is cybercrime.[28] This has proven to be a challenge since they affect the consumer, the merchants, and also the government. The merchants may loss profit and trust of their customers due to such activities.[29] Most consumers do not trust the e-commerce since they have at one point, fallen victims to fraudster or

[23] Saini, Hemraji et al, (2012), 'Cyber-Crimes and their Impacts: A Review', 2(2), International Journal of Engineering Research and Applications, India.
[24] Demombynes Gabriel and Thegeya Aaron, (2012), "Kenya's Mobile Revolution and the Promise of Mobile Savings, Journal of Policy Research work, Kenya.
[25] Ibid 30
[26] Chayes Antonio, (2015), 'Borderless Wars: Civil Military Disorder and Legal Uncertainty', Cambridge University Press, United States of America.
[27] The Kenya Vision 2030.
[28] Ibid 24.
[29] Bill Morrow, (2012), "BYOD Security Challenges: Control and Protect your Most Sensitive Data," 12, Journal Network Security, California.

from the tales told concerning online transaction.[30] Despite the fact there is consumer awareness they still do not trust the system an example is Nigeria.

1.5. THEORETICAL FRAMEWORK

The arguments in this study are based on the theory of Routine Activists and the Opportunistic theory. The theories are discussed below.

1.5.1. Routine Activity Theory

Routine Activity theory majorly deals with the culture of individual, how they do certain things, the way they have adopted to the existing environment through time.[31] In this context we look at commerce. Initially the way forward for trade was barter trade.[32] This has developed to online marketing which has become the way of doing business. Many people have opted to conduct business online since its affordable to most[33]. With this in mind we have to consider how this theory has affected e-commerce in relation to cybercrime. This theory explores the today-today activity that an individual has opted to take part in.[34]

It is based on three factors [35] namely:

a. There must be an existence of a suitable target. A suitable target can be defined as persons who appear to be vulnerable and are suitable targets for crimes

[30] Shalhoub, Z.K, (2006),'Trust, privacy, and security in electronic business: the case of the GCC countries', 14(3) Information management & computer security, Saudi Arabia.
[31] Felson Marcus, (1987), 'Routine Activity: Crime Prevention in the Developing Metropolis', 25(4), Journal of Criminology, Southern California.
[32] Weber Bradford (2015), 'A Routine Activity Perspective: Online Victimization', 22(4) Journal of Financial Crime, Weber State University, Utah.
[33] Newman Graeme and R.V Clarke, (2003) Superhighway Robbery: Preventing E-commerce Crime, 1st Edition, Willan Publishers, United Kingdom.
[34] Durkhein Emile, (1993). "Ethics and the Sociology of Morals", 2nd Edition, Macmillan Company, New York.
[35] J Miler, (2006), 'Individual Offending, Routine Activity and Activity Settings' 50(3), Journal of Research in Crime and Delinquency, Temple University, Pennsylvania

b. There are inadequate measures which entail cyber security put in place which ought to protect the business but they do not serve their purpose, due to the fact that such measures are outdated or they are not enough.

c. A motivated cybercriminal who has the intention and is motivated to commit a crime.

It argues that for a one to commit a crime, they will have assessed the issue at hand and then decide whether they would benefit from committing such a crime.[36] This process can be referred as the *rational choice theory.*[37] This theory enables on to understand how the cybercriminal make choices using the existing factors at hand. The individual who commit cybercrime are well known to have discovered the risk involved and assessed the situation in order to counteract in a way that they will not be caught if they decide to commit a crime.[38]

Consumers are vulnerable to cybercrimes because of the situation that they are in as internet users.[39] It is arguable that exposure to cybercrime majorly depends on the activity of an individual, such as banking, payment of bills, personal affairs and many other activities. Most individuals have literary become dependent on the internet based on the ease and services that they get.[40] They have changed the routine of doing things. E-commerce has created a platform for several users; they go online and shop at the same time attracting cybercriminals, making them a target.[41] E-commerce is the norm of today's business and thus more users become more dependent on it. The continuous use of the internet has fueled more criminal's activities.[42] Many people fall victim to cybercrime because they assume or don't take into consideration the risks involved and how

[36] Feslon Marcus and Boba Rachel, (2010), 'Crime and Everyday Life: Sociology Criminology', 5th Edition, SAGE Publications Inc. Texas State University, United States of America.
[37] Willison Robert and Backhouse James (2006), 'Opportunity for Computer Crime: Considering System Risk from a Criminal Perspective', 15 (11) European Journal of Information System, Australia.
[38] C. Smith et al, (2011) 'Cybercrime and On-line Safety in Cyberspace', 6(10) Journal of Criminology, New York.
[39] Peiravi Ali and Peiravi Mehdi, (2010),'Internet Security: Cybercrime Paradox' 6(1), Journal of American Science, Iran.
[40] Pedneault A and Beauregard E, (2014),' Routine Activity and Time Use', 23(1), Journal of Social Science, Canada.
[41] SChmalleger Frank and Pittaro Michae, (2008), 'Crimes of the Internet: Routine Activity Theory', 1st Edition, Prentice-Hall Press Upper Saddle, United State of America.
[42]Festl R et al, (2013), Problematic Computer Game Use Among Adolescents, Younger and Older Adults, 108(3) Journal of Criminal Justice, Germany.

vulnerable they are as online shoppers.[43] This has made most of the individuals' victims of cybercrime. The lack of knowledge has made them suitable targets for cybercrime activities.[44]
It does not seem to include the issues of computer-enabled crime due to human interaction across the web. Routine activity theory focuses majorly on activities that are carried out via the internet. It does not consider the novelty of human interactions via the cyberspace and the nature of cybercrime.[45] It looks at the insider threat but not the intimate handler or the crime facilitator. This theory is only based on the fact of why cybercriminal involve them in criminal activity.[46]

1.6. RESEARCH QUESTIONS

1. What are some of the theories that encompass the development of trade technologically?
2. What are some of the current laws placed to protect such developments?
3. How effective are this laws in ensuring the protection of technological advancements on trade?
4. What are some of the possible solutions and recommendation that the government can put in place to curb malpractices arising from such advancements?

1.7. RESEARCH OBJECTIVES

1. To investigate the jurisprudential debate informing the status of technological advancements on trade and how it will relate to Kenya.
2. To investigate judicial approaches to cases involving malpractices in such advancements in Kenya.
3. To make a comparative analysis of judicial and legislative approaches to matters involving technological advancements on trade in other jurisdictions.

[43] Smith Russell and Grabosky Peter, (2001) 'Online Security Fraud', 9(1), Journal of Financial Crime, New Zealand.
[44] Hartel Charmaine, (2007), 'the Global Village: Online Cross- Cultural Communication and HRM', 14(1), International Journal of Cross Cultural Management, Australia.
[45] Bodford Jessica, (2016), 'Human-Computer Interaction', 6(3), Cyber Psychology Journal, United States of America.
[46] Thompson Rebecca et al (2017), 'Crime Science: An Interdisciplinary' 34(10), Journal Springer publishers, England.

1.8. JUSTIFICATION OF THE STUDY

The aim of this research is to attempt to address the challenges that most corporate persons and entities are facing currently with the incorporation of businesses into the current technological advancements. The research also tries to explain on the possible solutions that can be achieved if such advancements are to be mitigated now that there are limited laws put in place to curb instances of technological malpractices. It tends to balance the competing interests of persons in the corporate world and their freedom to conduct their business through online means without interference from external forces by listing the various rights such persons have over such interference.

HYPOTHESIS

The study bases on the following hypothesis

- ✓ Although security measures have been put in place to curb instances of moral violation among learners, such mechanisms have not proven to be efficient due to the high moral degradation among the youth

- ✓ Although security measures have been placed by e-commerce merchant to protect their businesses. They have proven to be inadequate since they do not achieve their intended purpose
- ✓ Technological advancement is the main challenge to the legal framework currently. The laws that have been formulated are inadequate in dealing with certain crimes relating to technological advancement.
- ✓ Technological advancement has brought about the loss of jobs and an increase in the rate of unemployment levels which has led to the widespread of crime and the invention of new crimes.

1.9. METHODOLOGY

The library is the main source that was used. Reference will be by use of the relevant statutes books, journals, international treaties and convention. The library proves to be a secondary source as we are majorly dealing with the impact of technological advancement on the law in Kenya and

how the government of Kenya has dealt with such issues. The library is insightful based on the fact that it has more resources relating to Kenya. With the current regulations and policies put in place due to the covid 19 pandemic, the online resources/ library will come in handy in handling of this research.

The research study in itself, the impact of technological advancement on the law advocates for the use of technological means in handling of business. The internet being a technological means comes in handy as it provides for international organizations and treaties that deal with such matters relating to technological development.

1.10. LIMITATIONS OF STUDY

Technological advancement refers to the scientific improvements made in the activities of man. With the development of e-commerce, there are more cases of cybercrime.[47] Several authors have written more concerning the subject of the research. In this thesis we look at the approach of different authors towards the research question. Some of their opinions may be used as preposition in this research

One author, Kshetri[48], elaborates on some of the issues that need to be considered when dealing with e-commerce. Cybercrime has developed due to the development of technology and e-commerce. E-commerce has taken over the human life. It being part of the human life has attracted more cybercriminal who choose to attack such sites to obtained profits. He elaborates that individuals have depended so much on technology, specifically e-commerce.[49] This has caused an overdependence on such thus becoming vulnerable. Most merchants have fallen victims to such people.[50] One of the ways of dealing with cybercrime is the use of digital signatures which is contained in Section 3 of the IT legislation of India (2008)[51] .It is used to authenticate the electronic transaction. In addition there is need to give it a digital signature certificate so as to validate it. He goes ahead to discuss on issues relating to e-governance. He stipulates that e-governance majorly

[47] Chouhan Raksha, (2014), 'Cybercrimes: Evolution, Detection and Future Challenges' The IUP Journal of Information Technology, Hyderabad.
[48] Kshetri N, (2010) 'Global Cybercrime Industry, Economic, Institutional and Strategic Perspectives', second Edition, Springer, United State of America.
[49] Camqc Nicholas (2008), 'Emerging Trends in Cyber Crime, 13th Annual Conference - New Technologies in Crime and Prosecution: Challenges and Opportunities', International Association of Prosecutors, Singapore.
[50] Ramachnadran Ganesan et al (2010), a novel digital envelope approach for a secure e- commerce channel, International Journal of Network Security, Odisha.
[51] Information Technology Act No 21 of 2000 , India , Section 3

deals with the issues of electronic governance and the legal regime dealing with e-commerce. He provides that there is need for legal recognition of e-commerce records that can help in achieving justice. The aspect of civil liability is brought forth in this book. He claims that data theft can be done by the employees, who are part of the organization. Company loose more profit to their employees who have decided to conduct themselves in a manner that is a hindrance to the growth of such company. He opines on how some of the merchants have opted not to refer cases to the law enforcement agencies the moment they fall victims to cybercriminals. This has impeded the growth of e-commerce. They are afraid of losing the trust of their customers or even loose them.[52]

1.11. CHAPTER BREAKDOWN

This dissertation is organized in the following chapters.

Chapter One: This chapter will provide the background to the study that serves as the introduction. It will also contain the problem statement, research questions and objectives, hypothesis, theoretical framework, literature review, justification of the research as well as the research design and methodology

Chapter Two: This chapter will carry out a theoretical analysis around the impact of technological advancements on trade in relation to the law, its place in philosophy and its proponents. It will also include contrarian views to the same.

Chapter Three: This chapter tries to balance the rights of individuals and the measures placed to deal with technological crimes.

Chapter Four: This chapter entails a comparative analysis of judicial and legislative approaches to technological advancements on trade in other nations in order to draw important mechanisms for improvement of Kenya's laws and policies.

Chapter Five: This chapter will review the findings and make a determination on the legal effect of laws and measures that can be put in place to curb such instances of technological crimes on trade in Kenya.

[52] Geeta Virju, (2011), online identity theft-an Indian perspective, 18(3), Journal of Financial Crime, Emerald Group Publishing Ltd. India.

CHAPTER TWO

2.0 Theoretical Analysis

2.1 Introduction

Online trading is competitive in nature in that the merchants are expected to adapt to the changing market.[53] Online trading has changed the usual routine of handling businesses, making trading easy and open to many individuals. There are a myriad of challenges that have also developed as a result of this trade.[54] This paper will attempt to investigate and also analyses why online trading is not as successful as it ought to be. The following theories try to explain why there is rampant increase of crimes in the online markets and why many merchants have fallen victims to such crimes.

2.2 Routine Activity Theory

Routine Activity theory majorly deals with the culture of individuals, how they do certain things and the way they have adopted to the existing environment through time.[55] In this context we look at commerce. Initially the way forward for commerce was barter trade.[56] This has developed to e-commerce, an online trading platform which has become the way of doing business. Many people have opted to conduct business online since its affordable to most[57]. With this in mind we have to

[53] Sahin Cigdem, (2012), 'Competitiveness of E-commerce Companies: An Integrated Approach', 4(1), International Journal of E-business and E-government Studies, University of Victoria, Canada.
[54] Stratton Greg et al, (2016), 'Crime and Justice in Digital Society: Towards a 'Digital Criminology'?6(2), Journal of Crime Justice, Australia.
[55] Felson Marcus, (1987), 'Routine Activity: Crime Prevention in the Developing Metropolis', 25(4), Journal of Criminology, Southern California.
[56] Weber Bradford (2015), 'A Routine Activity Perspective: Online Victimization', 22(4) Journal of Financial Crime, Weber State University, Utah.
[57] Newman Graeme and R.V Clarke, (2003) Superhighway Robbery: Preventing E-commerce Crime, 1st Edition, Willan Publishers, United Kingdom.

consider how this theory has affected e-commerce in relation to cybercrime. This theory explores the everyday activity which individuals partake.[58]

It is based on three factors [59] namely:

a. There must be an existence of a suitable target. A suitable target are persons who appear to be vulnerable and are suitable targets for crimes
b. There are inadequate measures which entail cyber security put in place which ought to protect the business but they do not serve their purpose, due to the fact that such measures are outdated or they are not enough.
c. A motivated cybercriminal who has the intention and is motivated to commit a crime.

It argues that for a one to commit a crime, they will have assessed the issue at hand and then decide whether they would benefit from committing such a crime.[60] This process can be referred as the *rational choice theory.*[61] This theory enables on to understand how the cybercriminal make choices using the existing factors at hand.

Consumers are vulnerable to cybercrimes because of the situation that they are in as internet users.[62] E-commerce is the norm of today's business and thus more users become more dependent on it. The continuous use of the internet has fueled more criminal's activities.[63] Many people fall victim to cybercrime because they assume or don't take into consideration the risks involved and

[58] Durkhein Emile, (1993). "Ethics and the Sociology of Morals", 2nd Edition, Macmillan Company, New York.
[59] J Miler, (2006), 'Individual Offending, Routine Activity and Activity Settings' 50(3), Journal of Research in Crime and Delinquency, Temple University, Pennsylvania
[60] Feslon Marcus and Boba Rachel, (2010), 'Crime and Everyday Life: Sociology Criminology', 5th Edition, SAGE Publications Inc. Texas State University, United States of America.
[61] Willison Robert and Backhouse James (2006), 'Opportunity for Computer Crime: Considering System Risk from a Criminal Perspective', 15 (11) European Journal of Information System, Australia.
[62] Peiravi Ali and Peiravi Mehdi, (2010),'Internet Security: Cybercrime Paradox' 6(1), Journal of American Science, Iran.
[63] Festl R et al, (2013), Problematic Computer Game Use Among Adolescents, Younger and Older Adults, 108(3) Journal of Criminal Justice, Germany.

how vulnerable they are as online shoppers.[64] This has made most of the individuals' victims of cybercrime. The lack of knowledge has made them suitable targets for cybercrime activities.[65] This theory is only based on the fact of why cybercriminal involve them in criminal activity.[66]

From the above illustration it can be indicated that the way internet users go about their daily activity can have different impact on criminal activity. This theory is also closely related to opportunity theory which is discussed below

2.3 Opportunity theory

The routine theory operates on the basis of the opportunity available within the online marketing platform.[67] Online marketing has created a platform that allows individuals to carry out businesses without much capital needed to establish it.[68] This opportunity has not only attracted e-merchants but also criminals and fraudsters who exploit it.[69] Many measures are taken by individuals within e-commerce, but at the same time they tend to disregard the adverse risks that are there. The optimal level of security investment depends on the marginal cost and security benefits that the firm will incur.[70] Global connectivity[71] has enabled individuals to connect throughout the world. The interaction between individuals has changed widely over time. Obtaining products can easily

[64] Smith Russell and Grabosky Peter, (2001) 'Online Security Fraud', 9(1), Journal of Financial Crime, New Zealand.
[65] Hartel Charmaine, (2007), 'the Global Village: Online Cross- Cultural Communication and HRM', 14(1), International Journal of Cross Cultural Management, Australia.
[66] Thompson Rebecca et al (2017), 'Crime Science: An Interdisciplinary' 34(10), Journal Springer publishers, England.
[67] Lincke Susan and Green David, (2012) 'Combating IS Fraud: A Teaching Case Study', 6(1), Journal of Information System, United State of America.
[68] Cohen Sandra and Kalliroi, (2006) 'E-commerce Investments from an SME Perspective: Benefits and Processes', 9(2), The Electronic Journal Information System Evaluation, Greece.
[69] Lugo Mellisa, (2013) 'Self-control, Attitudinal Believes and White-Collar Crime Intentions', 12(5) Journal of Criminology, South Florida.
[70] LA Gordon, (2013), 'Investing in Cyber Security: Insights from the Gordon-Loeb Model', 7(48), Journal of Information Security, United States of America.
[71] Ewers Michael and Franzmeier, (2016), 'Left Prefrontal Global Connectivity: Cognitive Reserve in Alzheimer's disease', 12(7), Journal of Alzheimer, Israel.

be done by one key stroke.[72] This has created an opportunity to cybercriminals to exploit to the fullest.[73]

Business culture is another issue that is dealt with under this theory.[74] It deals with how the organization is managed. It starts from the resources available to the employee[75]Most of the organizations have failed to employ the basic controls that will ensure that the business is protected. Such loopholes make them prone to cybercrime.[76] The loopholes created within the organization have proven to be a perfect opportunity to be infiltrated by the insiders, who are the employees of the organization.[77]

Crime transverse between location, time and target this is the opportunity that are employed to commit a crime.[78] The internet has provided platform that allows the cybercriminal to exploit such factors. The fact the internet is readily for use has attracted more users.[79] More people have opted to use the internet for their activities and carry on business. When technology was introduced in the market, a few people could only afford them. The prices were reduces thus bringing as to the second stage. Many people decide to invest more in technology thus increasing its growth. It is at this stage that cybercrime developed.[80] The technology came with certain e-risks which individuals

[72] Khurana Anil and Mehra Jyoti (2007),'E-commerce: Opportunity and Challenges' 58(12), International Journal of Business and Management, Haryana, India.
[73] Dr. Franco and Regi Bulomine, (2016),'Advantages and Challenges of E-commerce Customers and Business: In Indian Perspective', 4(3), International Journal of Research, India.
[74] Sinkovics RR, (2007), 'Cultural Adaptation in Cross Border E-commerce' 8(4), Journal of Electronic Commerce Research, Germany.
[75] J Braithwaite, (1989) 'The Seriousness of Offenses: An Evaluation of Offenders and Non-offenders', 66(4), Journal of Criminal law, Australia.
[76] Choo Raymond, (2011),' the Cyber Threat Landscape: Challenges and Future Research Directions', 30(9), Journal of Computer and Security, University of South Australia.
[77] Willison R et al (2009)' Overcoming the Insider: Reducing Employees Crime Through Situational Crime Prevention, ACM publishers, India
[78] Ibid 29 Gibbson Stephen.
[79] Labrecque Li et al, (2013),' Consumer Power: Evolution in the Digital Age' 27(7), Journal of Interactive Marketing, Chicago.
[80] Mendoza Doris (2017) 'the Vulnerability of Cyberspace: The Cybercrime', 4(6), Journal of Forensic Science and Criminal Investigation, Philippines.

were aware of. The cybercriminals exploited this since its growth provided an opportunity for them.[81] Many studies have been conducted outside and within the United States; it has proven that opportunity is a significant factor for the commission of crime to occur.[82] Opportunity establishes itself in several ways and this motivates an individual to commit a crime.[83] Routine theory has raised a question on how to minimize the opportunities that are created due to the loopholes within cyberspace. The following are the recommended proposal to ensure the reduction of opportunities.[84]

a. The removal of criminal behaviors. Most criminals are attracted by the opportunities available. If the opportunity is reduced, then the lesser the criminals. This in turn will reduce the number of criminals within cyberspace.
b. Reduction in potential rewards and the factors that invite criminal activities. Most cybercriminals get involved in cybercrime activities due to the rewards that they get. There is need to ensure that the specific individuals are the only one ones who benefit from the online activity by ensuring such sites require authentication and
c. Increase awareness on the risks of crime

Opportunity theory is relevant in this research as it explains the ambiguities that are created with e-commerce. It provides a clear understanding on how cybercriminal use such to commit crime. For this to be dealt with there is need to ensure that such opportunities are reduced.

2.4 Technology theory

[81] Felson Marcus, Clarke Ronald, (1998),' Opportunity Makes the Thief: Practical Theory for Crime Prevention', Butterworth Publishers, London.
[82]Ulmer Jeffrey et al, (2001), 'The Age and Crime Relationship: Social Variation and Explanation', 107(4), American Journal of Sociology, Pennsylvania State University.
[83] Ibid 42.
[84] Gibbs Stephen, (2010) 'Applying the Theory and Technique of Situational Criminology to Counterinsurgency Operations: Reducing Insurgency through Situational Operation, 56(7), International Journal of Environmental and Situational Criminology, United States of America.

Technology is one of the objects that run the world[85]. It is readily available[86] According to the world Economic Forum Risk Report 2012 stated that about 470 million smartphones were sold, the number was also projected in 2015. Smartphone market expected to grow 55% in 2011 and approach shipment of one billion, International CorporationE-commerce cannot be carried out without considering technological factors.[87] For e-commerce to succeed there is need to establish that the technology itself is internet based and can be accessed.[88] Most merchants strive to obtain the best technology considering the profits that they will get. The need to have the best technology to carry out their business has driven merchants to invest more in acquiring the best technology. The question that arise is how prepared they for the new challenges are that may arise out of the new technology?[89] Nothing has been created to perfection.

It entails both the internal and external technologies which include the technology a firm uses and the culture of the firm.[90] Culture of the firm basically deals with intellectual resources.[91] A firm has to ensure that they have employed the best human resources who will enable the business to achieve its objectives at the same time ensuring that the business is protected.[92]

[85] Hajli Nick et al, (2015),'E-commerce Advancement and Technologies: Fueling the Sharing Commerce', 13(3), Journal of Technological Forecasting and Social Change, Swansea University.
[86] M.A Sasse et al (2001)'Transforming the "Weakest Link"- A Human/ Computer Interaction Approach to Usable and Effective Security '19(9), Journal of Technology, United Kingdom.
[87] Steward S et al (2003), 'The E-Commerce Revolution', 17(3), BT Technology Journal, United States of America.
[88] Martnez Candace and Williams Christopher (2010) 'National Institutions, Entrepreneurship and Global ICT Adoption: A Cross-Country Test of Competing Theory', 11(1), Journal of Electronic Commerce Research, Amsterdam.
[89] Raymond Louis et al (2004),' Cyber Entrepreneurship: A Multiple Case Study', 10(4), International Journal of Entrepreneurial Behavior and Research, Canada.
[90] Laudon K. and Loudon J, (2006), 'Management Information System: Managing the Digital Firm, 9th Edition, Prentice Hall Publishers, United States of America.
[91] Hasan Al-Mamary et al, (2014), 'The Meaning of Management Information System: Its Role in Telecommunication Companies in Yemen', 20(2), American Journal of Software Engineering, Yemen.
[92] Odumesi John, (2014), 'A Socio-Technological Analysis of Cybercrime: Cyber Security in Nigeria', 6(3), International Journal of Sociology and Anthropology, Nigeria.

CHAPTER 3

3.0 Legal Framework

3.1 Introduction

Kenya like other countries has been faced with issues that arise from e- marketing. E marketing has developed as a result of development within the cyberspace. The Internet has been transformed to perform an array of activities including trade. With the development of trade from the physical buying and selling of goods to the online form of trade, the legal framework has been tasked with the responsibility of trying to address irregularities and maintain order in such form of trade. For instance, cyber legislation has been developed to address such matters. Such legislation is meant to regulate transactions carried out within the country and beyond its borders.

Cyber security is an essential aspect when dealing with e- marketing.[93] It seeks to protect and develop the ICT infrastructure which is crucial to a country's economy. It does so through the adoption of appropriate legislation that is to oversee cyber related activities. This means that it goes ahead to provide measures of dealing with cyber related crimes and provide standards of carrying out online trading without an interference with the law. In addition, it addresses cyber issues and the loopholes within cyberspace.[94]

In Kenya, there exists a cyber-security strategy plan that is used to address cyber related issues.[95] The strategy affirms that there is need to work with other organization so as to ensure that there is maximum protection. With the introduction of policies such as the National ICT Policy which is meant to ensure that the concept of right based language is considered.[96] The same is emphasized in the Computer and Cybercrime Bill of 2016 which tries to balance the rights of individuals and the measures placed to deal with cyber related crimes.

3.2. Historical background of the Kenya ICT Policy

Kenya's economy has been boosted with the introduction of online marketing. This platform has been efficient in ensuring that market products are traded far and wide with the display of such

[93] Osborn Henry and Alexander Martin-Odoom, (2012), 'Fighting Cybercrime in Africa: Cyber Security', 2(6), International Journal of Computer Science and Engineering, University of Ghana.
[94] Tonge Atul et al, (2013), 'Cyber Security: Challenges for Society- Literature Review', 12(2), IOSR Journal of Computer Engineering, Section 27 (d) of the Critical Infrastructure Protection Bill 2016
[95] National Cyber Security Strategy (2014), Ministry of Information, Communication and Technology.
[96] National Information and Communication Technology of 2016.

products online. As a result, most users have been able to access such products because of the wide use of the internet in carrying out activities. The Kenyan government has made this possible by the introduction of an ICT related policy whose main objective is to encourage and increase investment in the internet and technology hardware.[97] The government has also gone ahead to establish legislations that govern e-commerce, to train and encourage individuals to participate more in e-commerce.

Due to such developments in commerce it led to the establishment of the *Communication Authority of Kenya* whose main functions are stipulated under the Kenya Information and communication act,[98] to include**:**

a) facilitate e-transactions,
b) Eliminate barriers such as uncertainties on writing and signature requirements,
c) Promoting public confidence, integrity and reliability of e-records and e-transactions and
d) Foster development of e-commerce in any electronic medium and develop sound frameworks to minimize forgery and fraud in e-commerce.

Section 5(4) of the Act[99] dictates the Authority in the performance of its purposes; to have regard to any policy guidelines and Kenya's responsibilities under any international treaty or agreement concerning the provisions of telecommunication, radio and postal service.[100]

The Act improved the regulatory latitude and jurisdiction of the Authority, and successfully altered it into a joined watchdog especially with regard to e-marketing. It took into account the guidelines for consumer protection in the context of electronic commerce of 2000. Some of the legislations that are incorporated within the laws of Kenya include:

a) EAC Legal Framework for Cyber laws 2008;
b) UNCITRAL Model Law on Electronic Commerce;
c) The 2005 United Nations Convention on the use of Electronic Communications in International Contracts and,
d) OECD Guidelines among other international treaties or agreements

[97] Section 3 of Cap 411A.
[98] Section 5 of Cap 411A.
[99] Section 5(4) of Cap 411A.
[100] https://ca.go.ke/industry/cyber-security/overview <accessed on 5th December 2018.

The National Kenya Computer Incident Response Team-Coordination Centre[101]

CAK is mandated by the Kenya Communication Act to establish a national cyber security strategy that will help in dealing with certain cyber related issues.[102] They created the National Kenya Computer Incident Response Team Coordination Centre whose main aim was to respond to any cyber security issues within the state of Kenya. In addition, it maintains awareness on cyber security activities.

EAC Legal Framework for Cyber laws 2008

EAC adopted a harmonized framework for cyber law in 2009. Its main goal is to integrate and regulate regional e-commerce through co-operation of the east African communities.[103] With its main function it created an EAC task force on cyber law that was granted the mandate to deal with issues related with cyberspace. They worked hand in hand with UNCTAD to ensure efficiency.

UNCITRAL Model Law on Electronic Commerce

The united nation commission was the one who developed the model law for e-commerce which has now been now adopted by Kenya within its legislation. The model laws were meant to harmonize the international trade laws so as to remove any obstacle that will hinder trade. It adopted the functional equivalence theory.[104]

The 2005 United Nations Convention on the use of Electronic Communications in International Contracts

It's an international instrument that is used to govern electronic transaction. [105]The purpose of the convention is to offer solution to any issues related to e-commerce.[106] The convention majorly concerns itself with international contracts. It entails the essentials required for online trade to be considered as a form of a contract. It seeks to promote certainty and predictability in

[101] Herein reffered to as KE-CIRT/CC
[102] Section 5B of Cap 411A.
[103] Article 5(1) East African Community Treaty.
[104] Ibid 268.
[105] The General Assembly adopted it on 23 November 2005 by resolution 60/21 and was opened for signature on 16 January 2006.
[106] Article 8 of the Convention.

international contract, enhance the principles of non-discrimination, technological neutrality which are the core principles of e-marketing.[107]

Consumer Protection Act and OECD Guidelines

E-marketing is developing rapidly thus becoming a main concern for the OECD.[108] The OECD guidelines are there to ensure contracts between sellers and consumers don't have any uncertainty. This is based on the theory of functional Equivalence. The consumer's rights are contained in the Consumer Protection Act[109]. The Kenya consumer protection act has envisaged some of the OECD guidelines which form the basis of consumer protection.

The OECD guidelines include:[110]

a) Transparency and effective protection,
b) Fair business practice,
c) Business should provide precise and clear information for easier identification. This includes information concerning the good and services. This will enable the consumers to make an informed decision based on such information,
d) Ensure that the payment mechanisms are secure and
e) Issues revolving around the dispute resolution mechanism should be dealt with clearly. This comprises of the applicable law and jurisdiction that they are subject to.

The consumer protection act provides that the consumers are entitled to quality goods,[111] correct information concerning the goods so that they can make informed decision.[112]

[107] Article 16 of the Convention.
[108] OECD (2015), Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document, OECD Publishing, Paris. http://dx.org./10.1787/9789264245471-en <accessed on October 27, 2018.
[109] Section 16(1) of the Consumer Protection Act, 2012.
[110] Guideline P 4 of the Recommendation of the OECD council concerning guidelines for consumer protection in the context of electronic commerce, guidelines (OECD recommendations).
[111] Section 7 of Consumer Protection Act, 2012.
[112] Saban Kenneth et al,(2002), A Critical Look at the Impact of Cybercrime on Consumer Internet Behavior, 10(2), Journal of Market Theory and Practice, Duquesne University.

3.3 Substantive law

3.3.1 Electronic transaction[113]

Electronic transaction exists between individuals who don't have a pre-existing relationship. Cybercriminals use this to their advantage as they can pose as either the seller or the buyer and obtain goods.[114] Hence the need for the law to come in.[115] The law has created a provision by introducing a compulsory electronic signature for any electronic transaction as Okuku puts it. This in turn has minimized chances of fraud.[116] The Kenyan statutes gives legal recognition to electronic forms of transaction.

3.3.2 Data protection and right to privacy

E-marketing requires merchants to provide vital and adequate information on the various trade websites for an efficient trade to take place. Data protection and consumers privacy work together to ensure that the consumers are protected as provided under the Kenyan constitution 2010 and the Draft National ICT.[117] This principle on privacy is also emphasized in the Data Protection Bill which provides supports that everyone has a right to privacy.[118] This also can be seen in the African Union Convention which ensures the protection of personal data.[119] From the above provision it's clear that the provisions try to ensure that the consumers are well protected and unauthorized data[120] access is considered as an offense.

It however has to be noted that there are no specific provisions that will guide one if faced with the question of privacy and cyber security.[121] In Kenya the act provides that an electronic record shall be secure at the time of verification[122].

---

[113] Article 1 0f the Africa Union Convention on Cyber Security and Personal Protection.
[114] Bray Jesse, (2016), Anonymity, Cybercrime and the Connection to Crypto-currency, 3(44), Criminology and Criminal Justice Journal, Eastern Kentucky University.
[115] Section 25 and 26 of the Computer Misuse and Cybercrime Act, No 5 of 2018
[116] Bello Marshal and Saulawa Abdullahi, (2015), the Relevance of Electronic Signature in Electronic Transaction: An Analysis of Legal Framework, Katsina State, Nigeria.
[117] http://techweez.com/2016/08/29/proposed-ict-policy-2016/< accessed on 26th October 2018.
[118] Article 22 of the Data Protection Bill 2016.
[119] Article 8 of the African Union Convention on Cyber Security and Personal Protection, 2000.
[120] Section 83U of Cap 411A.
[121] http://theconversation.com/kenyas-new-cybercrime-law-opens-the-door-to-privacy-violations-censorship-9727 < accessed on 4th December 2018.
[122] Section 83N of CAP 411A.

3.3.3 Digital evidence

It plays an important role in cybercrime investigation. Digital evidence in cybercrime challenges other traditional evidence.[123] E-marketing is an online transaction that allows an individual to transact via the internet. This means that all the evidence required in such a form of transaction is contained in the internet. Depending with the type of technology that one uses, most cybercriminals leave a digital print. The Kenya laws have addressed matters relating to electronic evidence.

3.3.3.1The Evidence Act and Electronic Commerce

The Act providers that electronic evidence is admissible[124] in court of law as long it meet the requirement provided under the act. This was demonstrated in the case *of* ***Republic v Barisa Wayu Mutuguda***[125] where the court went ahead to state that

"……*for electronic evidence to be deemed admissible it must be accompanied by a certificate in terms of section 106B (4). Such certificate must be in terms of S.106B (4) (d) be signed by a person holding a responsible position with respect to the management of the device.... Without the certificate this CD is inadmissible as evidence"*

***Nonny Gathoni Njenga and Another v Catherine Masitsa and Another*[126]**

In this case the main issue in contention was whether DVDs were admissible electronic evidence. The defendant referred to section 106 of the evidence act in his defense. He claimed that the DVD was obtained illegally and, constituting the infringement of his or her right to property, the DVD were not taken from one show but a series over a period time. The court held that the requirement by the law to ensure that electronic evidence is admissible was that there was need to accompany the evidence with certificate. Since this was the case the evidence was inadmissible

Another article in support of the evidence act is the Security Law (amendment) act of 2014 which allows for the admissibility of electronic evidence.

---

[123] Eogan Casey, (2002), 'Cyber Forensics: Error, Uncertainty, and Loss in Digital Evidence', 1(2), International Journal of Digital Evidence, Seattle.
[124] Section 106 of Cap 80.
[125] (2011) eKLR.
[126] HCCC No. 490 of 2013.

The fact that electronic evidence has been accepted in the court of law as admissible,[127] does not simplify the issue at hand. The evidence that ought to be deduced in court has proven hard to collect[128] with most of the electronic devices being wiped clean and their content deleted. This has reduced the chances of prosecuting certain individuals.

3.3.4 Intellectual property

Traditionally IPRs were considered to be territorial in nature.[129] Initially one had to exercise his rights in a physical form. For example a proprietor of a patent or a trademark has to ensure his rights in a particular country.[130] The internet has changed the whole concept as it made it hard to enforce such rights. It made IPRs boundless and extraterritorial in e-transactions.[131] The digital error has opened new opportunities allowing the creative industries to maximize their products it has also brought forth new challenges.[132] The distribution of information and product is done online.[133]Many individuals are able to access the material, copy and distribute them at a lower price.

3.3.5 Mode of payment and the lacuna in law

Online payment has been the mode of payment within e-commerce. Some of the e-marketers provide that payment is made before goods are delivered. In Kenya there are different avenues that are employed when it comes to online payment, such as Airtel Money and M-pesa. Cybercriminals have devised ways in which they can obtain personal information of customer account and use it to their own advantage to defraud the customers.[134] The consumer protection act recognizes that there are other modes of payment which may include credit cards.[135]

---

[127] Section 46 of the Computer Misuse and Cybercriem Act, No 5 of 2018.
[128] Makulilo Alex, (2008), Admissibility of Computer Evidence in Tanzania, 4(5), Digital Evidence and Electronic Signature Law Review Journal, Tanzania.
[129] Dr. Drahos Peter, (2002) the Universality of Intellectual Property Rights: Origins and Development, Journal of Economic History, United Kingdom.
[130] Kumar Anil, (2014), the Threat of Advancing Cybercrime in Organization: Awareness and Preventions, 5(8), International Journal of Advanced Research in Computer Science, Kenya.
[131] Kumar Arun, (2012), Issues of Cybercrime and IPR in Software Industry and Software Process Model, 44(1^0, International Journal of Computer Application, India.
[132] Balaji C, (2017), Role of IPR in Cyberspace, 2(5), International Journal of Advanced Educational Research, India.
[133] Castells Manuel, (2020), the Rise of the Network Society, 2nd Edition, Wiley-Blackwell, New Jersey.
[134] Ochieng Ray (2016), Cybercrime Trends in Learning Institution, International Journal of Education, Kenya.
[135] Section 1of the Consumer Protection Act NO.46 of 2012

3.3.6 Jurisdiction

This is the power that is granted to a court to hear and determine disputes.[136] Many courts have matters that fall within their jurisdiction. In this case the fact that cybercrime is extra territorial causes challenges.[137] The nature of cybercrime questions the jurisdiction of the courts to determine the matter in hand.[138] E-marketing has no geographical boundaries. [139]This is the same stand taken by the United Convention on Transnational Organized Crime.(UNTOC)[140]According to the laws of contract, the method of determining which law is applicable is based on the place where the contract took place or where it was performed.[141]If one is to be tried in a specific country then the court will apply the internal laws of that country.[142] At times the laws maybe unfavorable towards either one of the parties and justice may not be achieved.[143]

The internet has made this notion inapplicable. Cybercrime can be committed by an individual who is miles away and affects a different person in another country. The national laws have proven to be inadequate in dealing with such a vice[144]. There are no stipulations within the laws that show how to deal with cases that have a foreign element. This is an important aspect in e-commerce. The cybercriminals have used this as an advantage to continue their activity of depriving the merchants and consumer their profits and products respectively. [145]

There was a conference at The Hague on private international law[146] which was held solely for the purpose of addressing the issue of jurisdiction. The issue addressed was on of extra territorial jurisdiction, it suggests the adoption of two approaches: country of origin or country of

---

[136] Ibid 326.
[137] Dr. Azzam Adel , Jurisdiction in Cybercrim: A Comparative Study, 22 (3), Jouranl of Law, Policy and Globalization,Jordan.
[138] E. Elebeke _Why cybercrime thrives in Nigeria by Ewelukwa'13 April, 2011, Vanguard Newspapers. http://www.vanguardngr.com/2011/04/why-cyber-crime-thrives-in-nigeria-by-ewelukwa <accessed on 26th October 2018
[139] S.Snail (2013), Jurisdiction in Electronic Trans-Border Contracts, 4(2), Journal of Kwazulu-Natal Law Society, South Africa.
[140] Section 3 of the UNTOC.
[141] Brenner Susan and Koops Bert, (2004),' Approaches to Cybercrime Jurisdiction: Extraterritoriality and Extradition, 8(9), the Journal of High Technology Law, Suffolk University Law School.
[142] Rodriguez Teresa, (2010), Applicable Law and Jurisdiction in Electronic Contracts: Cybercrime, 45(10), International journal of Information and Technology, Mexico.
[143] Roux F, (2004), E-Commerce: The Legal Framework ', 19(6), Journal of Developing areas, South Africa.
[144] Ibid 335.
[145] Dr.Sagf Adel, (2014), 'Jurisdiction in Cybercrime: A Comparative Study', 22, Journal of Law, Policy and Globalization, Jordan.
[146] Loon VanHans, (2007), The Hague Conference on Private International Law,2(2), Hague Justice Journal, Rome.

destination.[147] Country of origin stipulates that the consumers are able to sue the offender within their country while the other one stipulates that one has to go to the offender's country and institute a suit there, upon which they will conform to the laws of the said country. The United States supported the country of origin approach while the other European country supported the other approach. Kenya on the other hand did not make a stand on either of the approaches suggested.

The Kenya law provides that the court shall have jurisdiction over any cybercrime matter, if the acts were committed in Kenya.[148] For the court to have jurisdiction over such issues the following conditions must be met;[149]

- ✓ The person committing the act or omission is a Kenya citizen or is ordinarily a resident in Kenya
- ✓ The act committed is against a Kenyan citizen or property belonging to the government of Kenya outside Kenya
- ✓ The person who commits the act or omission, after the commission of the act is present in Kenya

This kind of territorial jurisdictions referred to as objective territoriality.[150]

3.4 Procedural law

One thing that is clear is the fight against cybercrime is not only based on substantive law. There is needed to ensure that there are laws that help with the fight against cybercrime.[151] It is not enough to say that such an act is an offence, there is need to ensure that there are certain laws that will guide the law enforcement in ensuring that the said person who committed the act has been brought to justice. For justice to be guarantee, investigations should be carried out to identify the person.[152] In addition to training and equipment, there is need to have procedural measures to help the law agencies to perform their work.

---

[147] Brenner Susan and Ber-Jaap Koops,(2015) , Approaches to Cybercrime Jurisdiction, Journal of High Technology Law,

[148] Section 60 (1) of the Computer and Cyber Bill Act, 2016.

[149] Section 66 (2) (a) and (b) of Computer and Cyber Bill Act, 2016.

[150] Brenner Susan and Koops Jaap (2004), Approaches to Cybercrime Jurisdiction. 4(1) Journal of High Technology Law, Netherlands.

[151] Aldesco Albert, (2002),'the Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime', 23(1), LOY. L. Entertainment Law Review, Las Angeles.

[152] Bazin Philippe, (2008), Outline of the French Law on Digital Evidence, (5), Digital Evidence and Electronic Signature Law Review, London.

CHAPTER FOUR

4.0 Comparative Analysis

4.1 Introduction

E – Marketing is a form of trade which has mainly developed as a result of the use of Internet. In the previous chapter we have solely concentrated on cyber legislations in Kenya. We have looked at how Kenya has been approaching the issues of cybercrimes in relation to e-marketing. In this chapter we will concern ourselves with other legislation of other countries. It will look at how such countries have approached the issues that have arisen from this form of trade and what legislations have been put in place in support of this form of trade. This chapter concerns itself with how effective such legislations have been in curbing crimes related to this form of trade. It provides an understanding of how certain countries have approached the problem and dealt with the nature of e-marketing. The study is based on three countries: South Africa, United Kingdom and Ghana.

4.2 South Africa

4.2.1 Introduction

Technological advancements have improved trade. It has moved the trade perspective to e-trade which entails online transaction. Individual are allowed to conduct business at the comfort of their homes.[153] This is one of the benefits that accrue to the online sellers and buyers, at the same time the challenge that they face is cybercrime which is becoming rampant over the internet.[154] For this to be dealt with there is need to have regulation within the state. Initially e-commerce was governed by the common law and statutory provisions.[155]

These laws were inadequate in the sense that it could not address all the matters that related to e-commerce which led to the promulgation of the Electronic Communication and transaction Act.[156]

In Narlis v South Africa Bank of Athens[157]

[153] Selyer Carla and Mugavo Chipo, (2017), An Instigation into the Impact of E-commerce, M-commerce and Modern Technology on the Translation on the Industry in South Africa, 2017(1) Journal of management and Administration, South Africa.
[154] Ntozintle Jobodwana, (2009), E-commerce and Mobile Commerce in South Africa: Regulatory Challenges, 4(4), Journal of International Commercial law and Technology, South Africa.
[155] Fawzia Cassim, (2009), Formulating Specific Legislation to Address the Growing Spectre of Cybercrime: A Comparative Study ', 12(4), Potchefstroom Electronic Law Journal, South Africa.
[156] Act 25 of 2002.
[157] 1976 (2) SA 573 (A).

This case was decided prior to the enactment of the Electronic Communication and Transaction Act.[158] The case involved admissibility of evidence. The court in its holding, decided that section 34 of the Civil Proceeding Evidence Act did not recognize the admissibility of a computer print-out as evidence. The act only limited itself based on the statement provided by person as evidence. A computer was not considered a person who can talk hence any computer-generated evidence was not accepted in the court.

4.2.2 The law

From this illustration it's clear that the legislation placed were inadequate in relation to e-governance.[159] The Electronic Communication and Transaction act become the primary legislation of South Africa in relation to Cyber related issues and matters relating to e-commerce. The act was later structured in a manner that is substantive to addresses cyber related issues. This acts' interpretation Clause however still provides that the common law or any other statutes are still applicable and binding.[160] This is evident in situations where the act is not clear. This act works hand in hand with the UNCITRAL MLEC[161] which was adopted in 1996 whose main aim was to ensure that all contracts are verified and validated[162] and UNCITRAL MLES.[163]

Chapter III provides for legal requirement of electronic transaction. It provides that a data message need to be in writing and signed.[164] In addition, it prohibits discrimination of data messages by virtue of their forms.[165] It provides the legal ground for the admissibility of the data messages.[166] Matters involving signatures are comprehensively explained under the act.[167] It has established two tests for signatures of electronic transaction. These tests are used to ensure certainty and

[158] Here in Referred to as ECT Act.
[159] Swales Lee, (2018), an Analysis of the Regulatory Environment Governing Hearsay Evidence in South Africa: Suggestion for Reforms, http://journals.assaf.org.za/index.php/per/aricle/view/2916
[160] Section 3 of the ECT Act.
[161] The United Nation's Commission of International Trade Law (UNCITRAL) Model Law on Electronic Commerce (MLEC).
[162] Article 15 of the UNCITRAL MLEC.
[163] The United Nation's Commission of International Trade Law (UNCITRAL) Model Law on Electronic Signatures (MLES).
[164] Section 1 ECT Act.
[165] Section 11 ECT Act.
[166] Section 11 (1) ECT Act.
[167] Section 13 ECT Act.

enhance security in electronic transactions. The first test includes identifying a party and their approval[168] while the second test verifies the technology employed during the transactions.[169]

In addition, section 14 of the Act provides for the certainty of data messages. The requirements include:

a) The data message has not changed. Its integrity is intact, in that the original message and the finale message are the same[170]
b) The information is presentable to the interested parties[171]

Admissibility of such evidence in a court of law is covered under article 15, which sets out the conditions for any data message to be admissible as evidence in a court of law.[172] These provisions include reliability of the data based on how it was generated and maintained throughout the transaction.[173]

South Africa in curbing matters relating to cybercrime, they established an office of the cyber inspectors,[174] who are granted the mandate to inspect and monitor any website in the public domain,[175] in cases where they come across any criminal activity they have to report it. Accompanying these functions is the permission to search any premises prior to their investigation without notice and with a warrant to do so.[176]

Jurisdiction is one of the challenges that face cybercrimes. Section 90 of the act offers a solution to jurisdiction and sets the following standards for jurisdiction to be met;

a) The offense must have been committed within the republic of south Africa;
b) Any preparation toward the offense or part of the offense was committed within the republic, or where the results of the offense had effect within the republic;
c) Offense was committed by a South Africa citizen or a person with permanent residence in the republic or by a person carrying on business in the republic;

[168] Section 13 (3) (a) ECT Act.
[169] Section 13 (3) (a) ECT Act.
[170] Section 14 (1) and (2) of the ECT Act.
[171] Section 14 (1) (b) of ECT Act.
[172] Section 15 (1) (a) of ECT Act.
[173] Section 15 (1) (b) ECT Act.
[174] Section 80 of ECT Act.
[175] Section 81 -84 of ECT Act.
[176] Section 81 (1) of ECT Act.

In addressing the issue of jurisdiction bestowed upon the court, the act addresses the issues related to crime that are launched via third countries.[177] It provides that as long as the effects are felt in South Africa, the court have been granted the power to bring Justice to Victims. [178] Likewise, the courts are granted jurisdiction of all its citizens including permanent residents' holder and persons conducting business within South Africa irrespective of their location.

4.2.3 Implementation

The fact that the act has empowered the cyber inspectors to access and inspect houses is infringement to the right of privacy which is a provision in the constitution of South Africa.[179] The officers are to obtain information from the premises that is detrimental to the ongoing investigation. It argues that everyone has the right to privacy.[180] It can be clearly acknowledged that the ECT act has provided penalties for anyone who commits a cyber-offense. [181]The criminal sanctions imposed have been criticized to be inadequate as they do not deter any one from committing cybercrime.[182] On the other hand the Regulation of Interception of Communications and Provision of Communication-Related Information Act[183] is well known for providing severe penalties.[184] For example it provides for fines not exceeding R2 000 000 or imprisonment not exceeding ten years.[185] For Jurist the fine may be up-to R5 000 000 while the ECT Act provides for a maximum of five years.

In R v Douvenga [186]

The accused was an employee of an insurance company. She was found guilty of a contravention of Section 86(1) read with section 1, 51 and 85 of the ECT Act. It was alleged that the accused had intentionally gained entry to data which she had no access to, she knew that the data contained confidential information but still went ahead and attempted to send the data to her ex-fiancée via

[177] S Snail, (2016), Cybercrime and Cyber security in Africa –with an emphasis of on Cyber Terrorism and Cyber Warfare from a South African Perspective, Journal of Information, Law and Technology, Pretoria.
[178] Section 90 (b) of ECT Act.
[179] Section 14 of the Constitution of the Republic of South Africa, 1996.
[180] Delrae Goodburn, and Ngoye Martha (2004), Privacy and the Internet: The Law of the Internet in South Africa, first Edition, Van Schaik Publishers, South Africa.
[181] Reinhardt Buys (2004), Cyber Law, 2nd Edition, Van Schaik Publishers, Pretoria, SA.
[182] Ibid 361.
[183] Herein referred to as RICA.
[184] Section 70 of RICA.
[185] Section 50 of RICA.
[186] Case No 111/150/2003, 19th August 2003, Unreported.

e-mail. She had accessed over 30,000 names and addresses which she intended to go and use at her new place of employment. She was found guilty and charged with a fine of R1 000.

The criticism that arose in this case is the fine that was imposed by the court was less and yet the kind of damage that was done was beyond measure. [187]

Secondly there is the issue of jurisdiction.[188] The act has provided positive provision towards addressing the issue of cybercrime jurisdiction. Its provision includes the act that are committed by perpetrators who are abroad and the effects are being felt within the country;[189] the court has jurisdiction of all its citizens including the ones with permanent residency. This aspect of jurisdiction has provided a wide coverage of cybercrime.[190] Despite this being a positive step, in this case the section has overlooked the provision of the Magistrate court act.[191] It requires that the cause of action should take place in a certain court or district for it to have jurisdiction.

Evidence is crucial to every proceeding. The fact the act has provided steps to ensure that the evidence admissible in court has satisfied the admissibility of computer printout generated evidence. We acknowledge that the act recognizes the admissibility of computer print-out; it is grouped under the documentary evidence which has to pass through a different test to be admissible in court. These hurdles include: the original version rule; the authenticity rule and the hearsay rule.[192] Once the document satisfies such rule then it will be admissible in court. These rules however were not designed for computer printout. Computer printouts are data messages that have been obtained from a computer. The transactions mostly of the two individuals hence one cannot third party to be involved. There is need to ratify the provision of section 15 of the ECT act.

In Ndlovu v Minister of Correctional Facilities[193]

The applicant relied on two-page print out as evidence against the accused person. The court decided to subject the computer print out to the evidence rule, the print out was a copy, to determine

[187] Barton Paul and Nissanka Viv, (2003), Cybercrime: Criminal Offense or Civil Wrong? 19(5), Journal of Computer Law and Society Report, New Zealand.
[188] Reed Chris, (2004), Internet Law Text and Materials, 2nd Edition, Cambridge University Press, Cambridge.
[189] Hale Chris (2002), Cybercrime: Facts and Figures Concerning the Global Dilemma 18(65), International Journal of Crime and Justice, USA.
[190]SS Snail (2009), Cyber Crime in South Africa: Hacking, Cracking and Other Unlawful Activities ', 13(6), Journal of International Law and Technology, South Africa.
[191] Section 28 (1) (d) of the Magistrate Court Act, (Act 32 of 1944).
[192] Collier David, (2005), Evidently not so Simple Producing Computer Print-outs in Court,13(1), Juta 's Business Law Journal, University of Cape Town.
[193] 2006 (4) All SA 165 (W).

whether or not the print out may be admissible in a court of law. The accused objected the admissibility of such evidence based in the fact the document was not an original copy hence could not meet the evidence rule. The court in issuing its judgment relied on Section 3 0f the law of Evidence Amendment act opposed to Section 15 of the ECT act. Section 15 of the ECT Act is silent of the rule that should be used to clarify and verify electronic Evidence. This decision has been criticized as the main Act which ought to cover the Entirety of cybercrime has not done so.[194]

4.3 The United Kingdom

4.3.1 Introduction

The internet has penetrated the countries system of economy at a very fast speed. This has promoted the growth of e-commerce as most individual have decided to use the availability of the resources.[195] With such development, the country started experience challenges which were closely related to e-commerce. [196]Cybercrime has been one of the longest crimes that the United Kingdom has tried to curb for quite sometimes.[197] One of the organizations that have been affected by such is the SMEs who do not have the resources to curb such challenges.[198] In ensuring that they deal effectively with this matter the United Kingdom established a body that deals with such known as Serious and Organized Crime agency. In addition to this they established laws that can be used to regulate e-commerce transaction at the same time ensuring its protection. The organization was under the Serious and Organized Crime Act 2005.[199]

4.3.2 The law

The CMA is the main legislation that is used to deal with matters relating to cybercrimes. This act sought to address two main issues which include: the issues related to Dos attacks and the UK obligations for the commitment of fighting cybercrime especially with the ratification of the council of Europe convention on cybercrime.[200] The amendment of the act has brought forth

[194] Ibid 362.
[195] Pettigrew Andrew, (1985), the Awakening Giant, Blackwell Publishers, Oxford.
[196] Ibid 53 pettigrew
[197] Lagazio monica et al, (2014), a Multi-Level Approach to Understanding the Impact of Cybercrime on the Financial Sector, Journal of Computer and Security, London.
[198] Quayle Michael, (2002), E-Commerce: The Challenges for UK SMEs in the twenty- first Century, 22(10), International journal of Operation and Production Management, UK.
[199] Section 2 of the Serious and Organized Crime Act 2005.
[200] The amended section 1 of the Computer Misuse Act.

changes, such as the penalties for unauthorized access has been increased from six months to two years of imprisonment.[201] To curb the nuisance concerning cybercrime, the United Kingdom decided to take initiatives and established a body that comprised of the police, members from the private sector and the academics to come together and form a team considered as National High-Tech Crime Unit.[202] The main purpose for the establishment of such a unit is to ensure that the individuals work together as and come up with lucrative ways of dealing with cybercrime.[203]

4.3.2.1 Salient Features of the Act

The CMA provides that anyone who is able to access data without authorization shall be liable in relation to this act. [204] Personal data has been defined to be data that is held in a computer and contains information of individuals.[205] For one to be liable there is need to ensure that the person has satisfied the elements of criminal responsibility which entails: the Mens Rea and Actus Reus.[206] This is entailed in the act as they provide that the person must have the intention to commit such a crime thus someone will be said to be liable if such principles have been fulfilled. In addition, where someone has accessed the information and intends to use it to commit further offense then the individual shall be held liable according to the provision of section 2 of CMA. The laws also include the aspect of aiding and abetting. Where an individual obtains information and uses it to commit or intends to give it out so that it can be used to commit other offenses then they will be held liable.[207]

Issues related to internet jurisdiction are addressed by the act. The United Kingdom uses the principle of territoriality to address such issue.[208] It provides that in instances where the crime has been committed outside the UK, it still has jurisdiction to try the perpetrator under this act.[209] The act provides that it is not compulsory that the offense is committed within the territory of United

[201] Section 2 of the amended Computer Misuse Act.
[202] http://www.nationalcriemagency.gov.uk/about-us/what-we-do/national-cyber-criem-unit < accessed on 5th November 2018.
[203] MacEwan, (2008), The Computer Misuse Act 1990: Lessons from its past and Predictions for its future 'Criminal Law Review, (2008) 1-9, United Kingdom.
http://usir.salford.ac.uk/15815 accessed on 5th November, 2018.
[204] Section 1 of CMA.
[205] Section 1 of Data Protection Act 1998.
[206] Section 2 of CMA.
[207] Section 37 of the Police and Justice Act, 2006.
[208] Section 8 of the Official Secret Act, 1989.
[209] Section 3 of CMA.

Kingdom, just as long as the effects of such offense is felt within the state then the state shall have jurisdiction over the matter.[210]

4.3.3 Implementation

Section 1, of the CMA Act, deals with unauthorized access of computers. It majors itself with hackers on the face value but does not consider the circumstances where the hackers may be the employees within the business. This has been critiqued based on the fact that it doesn't seem to extend to cover the illegal act that the employees are involved in. In addition to this the UK is a member of the European Union thus in cases of deficiency in laws then the laws there are other laws that might supplement the existing laws of the country. They also adhere to the European Cybercrime Convention which stipulates for jurisdiction of cybercrime. The convention grants the parties to choose where the offense may be tried.[211]

In DPP V Bignell[212]

This case involved two officers who were authorized to obtain information from the police national computers. The information was to be used for police purposes. The officers requested for the information on different occasion and the police operator was obliged to give them the information they sought. Later on, it was discovered that the two police officers used the information for their own personal use. The court in its judgment held that the police did not act contrary to Section 1 of CMA act.

The criticism was based on the version that the purpose for authorization relied on the fact that, the information obtained shall be used for police work. Their action was contrary, the authorization limited the use of such information hence the fact that they obtained the information for personal use, means that they accessed information illegally. If one talks about unauthorized access this may include the employees too. As long as they work within the authority granted then it shall not be considered unauthorized access but if not, then there is need to ensure that such individuals are brought before the law. The court in their judgment in another case sought to clarify the standing that they took in Bignell's case.

This was in the case of ***R v Bow Street Magistrates Court and Allison***[213]

[210] Section 4 of CMA.
[211] Article 22 of the European Cybercrime Convection.
[212] 1988) 1 Cr. App. R. 1.
[213] Ex parte Government of the United States of America (Allison) [2002] 2 AC 216.

The House of Lords were faced with a question of whether an employee accessed information without authorization. The employee in this case used a computer to access data that she knew she was not entitled to. The court, in overseeing this case explained that the employee would be found guilty if the employer has limited the authority of the employee. In this instance the employee was not in violation of Section 1of CMA. Section 2 is more comprehensive based on the fact that it considers that the person intends to use the obtained data to commit other offenses.

Section 3 of the MCA is not working alone as the UK has signed an Extradition treaty with two other states that is the United States and Northern Ireland. The treaty is meant to supplement this act based on the fact that certain offenses may be tried by another state that has jurisdiction over the matter.[214]

In Gary McKinnon Case[215]

The accused person was a system administrator. He went ahead and hacked into the United States military and NASA computers from the comfort of his home. Once he had hacked the computers he deleted the data from the computer making the USA loose crucial information concerning its naval intelligence and weapons. Such actions left USA vulnerable to attacks as this hacking had affected the national security of the States. Once investigation had been carried out by the National High-tech unit he was apprehended as he was the perpetrator of the act. The extradition treaty signed between the UK and the USA, covered such offenses, the United States requested for the extradition of the accused person. His legal team argued that the accused person could not be extradited based on the fact that the act was committed in UK and the accused person was a citizen in that state. The court ruled that the extradition treaty put in place conferred jurisdiction upon the USA. In addition, if he was tried by the UK then the accused person would serve a lesser sentence as the penalty stipulated were less. Section 3 of the MCA cat proved that there was insufficient evidence since it was not established if the individual has any malicious intent.

The issue that has been raised is the aspect of the penalties that has been given.[216] The MCA provided for a minimum sentence of not more than five years. The aspect that the laws do not consider the havoc that the said individuals leave in their wake has raised some concerns.

[214] Article 2 of the Extradition treaty of 2003.
[215] (2008) UKHL 59.
[216] Sultan Ali, (2010), Combating Computer Crime: An International Perspective, Journal of Information Technology, Southern Queensland.

In the case of R v Simmo Vallor[217]

It involved a web designer who created a mass mail virus which he distributed all over the country. Over 70,000 individuals were affected by his action. The accused pleaded guilty in the court and was only sentenced to two years.

The law is there to ensure that they deter other individual from committing a crime but this is not the case as seen above. There is need to ensure that amendments are made in order to ensure that this law protects and uphold the deterrence principle.[218]

4.4Ghana

4.4.1 Introduction

Cybercrime is a new marvel in Ghana. It was experienced initially in the year 1999[219]. Throughout cybercrime has developed tremendously due to the development of internet.[220] One of the prominent cybercrime that has taken over Ghana is fraud there are many instances where the said citizens involve in activities that intent to defraud unknowing individuals.[221] This developed to the internet scamming activities.[222] The internet connectivity makes it easier for such individuals to carry out such activities.[223] Most victims are very reluctant to report such crime to the police and that's why cybercrime is developing.[224] Due to such scammers the Ghana government established the commercial crime unit which was helping the police to apprehend the financial scammers.[225] An example, of the most common group that has taken over the scamming industry is the Sakawa boys.

---

[217] 2003 EWCA Crim. 2288.

[218] Trend Micro, (2015), Punishing Cybercriminals: What do they Deserve? United Kingdom. https://blog.trendmicro.com/punishing-cyber-criminals-what-do-they-deserve/ < accessed on 6th November, 2018

[219] Warner Jason, (2011), Understanding Cybercrime in Ghana: A View from Below, International Journal of Cyber criminology, Ghana.

[220] Olunide Longe et al, (2010), Cybercrime and Criminality in Ghana: Its Forms and Implication 15(12), Journal of Information and Technology Ghana.

[221] Burrel Jenna, (2008), Problematic Empowerment: West Africa Internet Scammers as Strategic Heyday Publishers, California.

[222] David et al (2007), Current Trends in Advance Fee Fraud in West Africa, EFCC, Computer Security and Critical Information Journal, Nigeria.

[223] Perry Katy, (1992) travellers on the internet: a survey of internet users online 19(2), Electronic Networking Applications and Policy Journal., Ghana.

[224] Duah Francisca, (2013), The Growing Threat of Cybercrime: Implication for International Relations, Journal of Information and Technology, University of Ghana.

[225] Boateng Richard et al, (2011), Advancing E-commerce Beyond Readiness in a Developing Economy: Experiences of Ghanaian Firms, Journal of E-commerce in Organizations, Vancouver.

Sakawa boys [226]

This is one of the prevalent cybercrime that has taken over Ghana State. In 2010 the gem country had its name tarnished as it was mentioned as one of the countries that cybercrime is prevalent.[227] This case involved a young group of individual men who decided to fraud British and American men. Online dating is a business that has been carried on for ages. In this case the sakawa boys 'as they are referred to, took this to another level. They targeted the unknowing men who were searching for love online. They would pose as women online and shoplift photo of beautiful women and they proceed to chat with the American men. After some time of chatting and professing their love they would ask the men to send them money so that they would carter for their needs. Many men have fallen victim to such pranks. Arresting them has proven to be a bit difficult since the police do not have the required assistance that they need so as to ensure that such individuals have been brought to justice. This influenced the decision of Ghana to establish a commercial crime unit of the CUID of the Ghana Police Service which is tasked with the responsibility of investigating arresting and prosecuting anyone involved in internet fraud.[228]

To ensure that they curb such nuisance the country decided to come up with legislation that ensures that they deal with such issues. They developed the Electronic Transaction Act[229] which was adopted in 2008. This act provided a comprehensive understanding of cybercrime offenses and the issues relating to cybercrime.

4.4.2 The laws

The Electronic Transaction Act is the main legislation that is used to govern cyberspace. The act has been stipulated in order to address the country's issues that impede the economy which is in compliance with the Budapest convention.[230] It recognizes electronic evidence[231] which is considered as an electronic record. The act provides for condition that will allow the evidence to be admissible in a court of law to include: Relying on the originality of the document from which it was created or displayed, the courts have to consider the integrity of the document and the

[226] https://topdocumentaryfilms.com/sakawa-boys-internet-scamming-ghana < accessed on 6th November, 2018.
[227] Budu J. et al, The forms of cybercrime in Ghana, 11(2), Journal of Information Technology Impact, Ghana.
[228] Boeteng et al (2009), 'Developing Countries E-commerce Capabilities in Garment Manufacturing: The case of Ghanaian Firms, Pro-Write Publishers, Vancouver.
[229] Here in referred to as ETA.
[230] Article 15 of the Budapest Convection.
[231] Section 144 Electronic Transaction act.

manner in which the parties are identified in relation to the document. The admission of electronic evidence is not limited to the requirements of the act but also the requirement of Relevance is also an essential requirement as contained in the evidence act.[232]

Jurisdiction of cybercrime has been provided under section 142 of the act which provides that states shall have jurisdiction over cybercrime matters on the following instances:

- ✓ The accused person was in the country when the act was being committed;
- ✓ The computer used was located in the country this relates to matters of payment of money., the financial institution authorizing the payment is within the country and
- ✓ The offense occurred in Ghana.

4.4.3 Implementations

Despite the fact that there is stipulation of electronic evidence it has been hard to implement the requirement contained within the act. The act has stipulated the requirement that will be needed to ensure the admissibility of electronic evidence. The following cases will look at the effectiveness of the said provisions.

R v oler[233]

This case involved the integrity of a digital forensic with regards to maintenance of logs, records and certificate of inspection. The various records were officially handwritten, later on transferred in to the computer while other were captured in PDF form. The court had to consider the witnesses statement that had entered the information to the laptop. They considered if the information entered were the same as the one entered in the computer. It was discovered that the information obtained were not the same so the integrity of the document was compromised. The act recognizes the principles of statutes in relation to the admission of electronic evidence.[234]

The court under certain circumstance may not accept the electronic evidence. This has raised contra version based on the fact that they are electronic evidences which have been converted in manner that the court does not agree with it.[235]

In R v Alexander Tweneboah[236]

[232] Section 144-part IV ETA.0
[233] [2014] ABPC 130.
[234] Section 3 ETA.
[235] Goodchild Joan, (2009). "E-Commerce Fraud: The Latest Criminal Schemes," Network World journal, Chicago.
[236] Unreported ruling of the high court of Ghana, 9 June 2016) TB 15/13/1.

The case involved the admission of the accused emails as evidence in the court of law. The email contained illegal communication service known as Sim-boxing. The information was extracted from his laptop and stored in a compact disk. The evidence was inadmissible based on the fact that it did not adhere to the procedure stipulated in the act.

The decision of this court raised concerns on what entails electronic evidence. The act stipulates that the evidence should be in its original form. The court's interpretation of electronic evidence seems to lean on the side of documented evidence which causes biasness to some of the evidence and thus justice may not be achieved.

Another matter that is raised is the issue of the right to privacy. The court in its decision, tend to uphold this right and try to balance them with the existing offense. If the evidence was obtained due to the infringement of such aright the evidence may not be admissible in a court of laws.[237] The right to privacy is essential to every citizen and should be upheld.

Ackah v Agricultural Development Bank [238]

The court questioned the aspect of admissibility of evidence that was obtained by infringing the right of an individual it applied the doctrine of balance. The court stated that if a part's right is infringed while obtaining the evidence then, the evidence will not be admissible in a court of law. The court had to weigh the rights of the individual against the circumstances at hand.

It is missing key part of cybercrime, such as forgery. The ETA relates to traditional forgery that is covered by the Criminal Offenses Act, 1960. The ETA describes Cybercrime in the aspect of any computer related crime. The focus in the Ghanaian law is based on financial fraud and no other integral part of cybercrime such as illegal access.[239] Unauthorized access is one of the major ways an individual may obtained any information from a website. This has affected many individuals since they tend to lose more information to such practices. In governing such problems, the state uses the criminal act of 1960 which does not cover all the aspect of cybercrime.it majorly deals with corporal and property related issues. [240]

The key aspect of cybercrime is jurisdiction. In this act, the matter is limited as the act provides that state has jurisdiction over its citizens.[241] It provides that if the access was in the country or the

[237] Thomas David, (2003), A general inductive approach for qualitative data analysis, 27(2) American Journal of Evaluation University of Auckland.
[238] J4/31/2925) [2016] GHASC 49.
[239] Pati Dayal, (2003), Cybercrime, Universal Law Publishing Co, New Delhi.
[240] Section 158 of the Criminal Offences Act.
[241] Graham T (2002), 'Dispute resolution: E-Fraud and Jurisdiction, Winter Publishers, New York

medium through which the act was done is located the country then the court shall have jurisdiction. [242] In addition, the offense has occurred within the country. This is limited jurisdiction. This is ineffective provision that does not deal with the aspect of borderless and free location of cybercriminals.[243] If this stipulation is used to solve cybercrime then it will be hard since cybercriminals are located all over world and cybercrime can be committed anywhere.[244]

4.5 Comparative analysis

4.5.1 South Africa

The ECT Act is the main legislation that is used to govern issue related to cybercrimes. The act has provided for the recognition of electronic data and validity of data messages. The act also includes the definition of cybercrime under Chapter XII. This provision can be used as a guideline as to what necessitates to an electronic transaction. In addition, it ensures certainty of electronic transaction. One thing that has been outstanding practice is the permission granted to the cyber-inspectors to enter any premises without any permission.[245] This is in violation of the right of privacy[246] which is a constitutional right by virtue of the supremacy clause.[247] This is a demerit of the act as this law is considered invalid.

From the illustration provided above it can be said that the penalties provided for such offenses are minimal. If a penalty does not match the quantum of damage, then who are they punishing? There is need to ensure that the penalties place deter individual from committing the same acts. With this in mind, South Africa decided to amend the Electronic Communication and transaction act in matters relating to penalties. The amendment bill of 2012[248] seeks to increase the penalties provided for under section 86(2) from a maximum imprisonment of 12 months to 10 years. section 88 deals with anyone who aids and abets any act stipulated under this act shall be imprisoned for a maximum of 5 years or to pay a fine amounting to R5 000 000. This bill tries to carter for less penalties that were originally stipulated.

---

[242] Article 142 (2) ETA.
[243] Zuppo Colrain, (2012), Defining ICT in a Boundary Less World: The Development of a Working Hierarchy, 4(3), International Journal of Managing Information Technology, Maryland University College.
[244] Coomson Joseph, (2006), Cybercrimes in Ghana, Ghanaian Chronicle, Ghana.
[245] Section 82 ECT Act.
[246] Section 14 of the South African Constitution, 1996.
[247] Section 2 of the South Africa Constitution, 1996.Provides that the constitution is the supreme law; any other laws that is inconsistent with the constitution is invalid.
[248] Electronic Communications and Transactions Act Amendment Bill 2012.

Jurisdiction is an issue that a country may not overlook when it comes to e-commerce. It has provided for the condition that the courts have jurisdiction to hear the matter. The only thing that it left out is which court shall have the jurisdiction to deal with the issues. The provision of the act seems to clash with the provision of the Magistrate Court Act. The bone in contention is the additional jurisdiction conferred on the court in matter relating to the course of action involving abroad actions. The Magistrate Court act stipulates clearly which court has jurisdiction to hear the matter. It bases it principle of jurisdiction on where the action took place or the district.[249] The act does not give direction on how to approach eth matter or which court has the jurisdiction to hear and determine the matter. This is a disadvantage. Despite its shortcoming the act has tried to ensure that there is e-governance. Its function may not fully protect the individuals from cybercrime but it makes effort to try and ensure that cybercrime does not become rampant.

4.5.2 United Kingdom

As stated above the electronic computer misuse act is the one that is used to govern e-commerce activities. We can clearly see that the article that have been provided under this act have tried to expansively define what entails unauthorized within its definition. It tries to explain at what circumstances an individual may be assumed to have been in violation of the act. The minimum sentence for such activities is ten years.[250] In addition, these acts there is the amendment of section 3A of the act which now entails the use of such information in order to commit other crimes.[251] The United Kingdom is serious about dealing with the issues involving to cybercrime. It has been fighting cybercrime for a long period of time. With this being the case there is a proposed bill that will amend the act. The Serious crime bill was introduced on 2014. The purpose of this bill is to amend certain part of the CMA act by including the serious attack that will cause serious damage to individuals.[252] In addition to adding new offenses to the act the bill also looks at the penalties that have been given.[253] It aims at ensuring that the penalties equals to the quantum of damage caused.[254] The United Kingdom sees cybercrime as not just being committed by an individual. It

[249] Section 28 (1) (d) Magistrate Court Act.
[250] Section 2 CMA.
[251]Section 3 CMA.
[252] Solon Olivia, (2014),UK Law introduces Life Sentences for Cyber Criminals, 6th June, 2014. https://www.wired.co.uk/article/cybercrime-bill-life-sentence < accessed on 6th November 2018.
[253] The Serious Crime Bill and Related Material', Equality and Diversity Forum online issue of the 23rd October, 2014, http://www.edf.org.uk/the-serous-crime-bill-and-related-material/ <accessed on 6th November 2018.
[254] Ibid 467.

looks at cybercrime as a crime that is committed by an organized group. It is due to this that they have decided to launch an attack against the organized crime units.[255]

The approach that the United Kingdom has taken in matters relating to jurisdiction is an important step.[256] E-commerce is borderless so is cybercrime.[257] This approach is suitable as it does not limit itself to territorial boundaries. [258]They try to bring justice to all the victims. The signing of the extradition treaty also made it more applicable. This concept is essential in respect to e-commerce.[259] From the illustration above concerning CMA it can be said that the drafters considered the fact that cybercrime develops with time. The act has been effective since the 1900s and has been functioning as it easily adopts the changes that accrue within cybercrime. It considered that nature of cybercrime. This is an important part of the legislation as it will not be rendered inapplicable after sometime.[260] It was drafted broadly to cover the width of cybercrime. The one challenge that faces most legislation is the interpretation of the law. The judges who are interpreting the laws may at times interpret it in a manner that may not be right. This was illustrated in the case of, ***R v Cropp***[261] where the judge felt that the defendant would only be liable to have committed an offense if he had used one computer to access information from another computer. Despite all these, it can be said that the CMA act is on the right path as it tries to establish what unauthorized access in light of cybercrime is. The United Kingdom laws have tried to establish legislations which have proven to work when it comes to protection of individual from cyber-attacks.

[255] Burden Palmer et al, (2003), Cybercrime: A New Breed of Criminals? 19(30), International Journal of Computer Law and Security Report, Kent State university.
[256] Johnson David and Post David, (1996), Law and Borders: The Rise of Law in Cyberspace, 48, Stanford law review Journal, Chicago.
[257] Kshetri Nir, (2005), Pattern of Global Cyber War and Crime: A conceptual Framework,11(4), Journal of International Management, India.
[258] Pounder Coulson, (2001b), The Council of Europe Cybercrime Convention, 20, Journal of Computer and Security, Europe.
[259] Pounder Coulson, (2001a), Cybercrime the Backdrop to the Council of European Convention, 20, Journal of Computer and Security, Europe.
[260] Tyson Dave, (2007), Cybercrime: A Pervasive Threat, 81, Journal of Security convergence, USA.
[261] (1991) 3 Unreported.

4.5.3 Kenya

There are several legislations that have been made in order to govern cybercrime.[262] The main legislation that is used here is the Kenya Information and Communication Act. The act recognizes electronic transaction and one of the requirements is that they need to have signatures. This is an important aspect of e-commerce. Cybercrime has become rampant in Kenya[263] thus there is need to have electronic signatures for any transaction that is done via electronic means.[264] The penalties that have been provided for seem not to be enough to deter anyone from committing any crime. If one access data without any permission then they are only liable for not less than there year of imprisonment.[265]

Kenya is one of the developing countries hence may not have the resources required to deal with such issues.[266] This maybe contributed by the level of corruption within the country, poverty and other issues. [267] The law enforcement agencies are not well equipped to deal with cybercrime issues.[268] As we have seen from South Africa and United Kingdom, they have established bodies that specialize and focus only on cybercrime.[269] They have been granted the power to address all the issues of cybercrime. In addition to that they form part of the police force of the country. [270] If there are adequate personnel then it will be easier to curb such issues. In addition, the turn out of the victims who report the crimes has been low.[271] This is based on the fact that there are few cases that have been solved. If the country would emulate the steps that South Africa has taken to ensure that the law enforcement do not work alone when it comes to cybercrime this would have made it

[262] Kinyanjui Mary and McCormick Dorothy, (2002), E-commerce in the Garment Industry in Kenya usage, Obstacles and Policies, Institute for Development Studies Journal, University of Nairobi, Kenya.
[263] David Bell (2001), Cyber Culture: The Key Concepts Routledge Publishers, USA.
[264] Shemi, AP. (2012). Factors Affecting E-commerce Adoption in Small and Medium Enterprises: An Interpretive Study of Botswana. Unpublished PHD Thesis: Business School, University of Sanford, UK.
[265] Section 83x (2) of KICA
[266] Mutume Mandel, (2007), Organized Crime Targets Weak African States 21(2), African Renewal Journal, South Africa.
[267] Karake Zeinab and Qasim Lubna, (2010), Cyber law and Cyber Security in Developing and Emerging Economies, Edward Elgin publishing, Malaysia.
[268] Kenpankho P. et al (2005), The Obstacles of e-Commerce in developing countries, Proceedings of the International Conference on Computer and Industrial Management, ICIM. Bangkok, Thailand.
[269]Sommer Peter, (2004), the Future of the Policing of Cybercrime, 1, Journal of Fraud and Security, Britain.
[270] Ibid 483.
[271] Giddens Anthony, (1990), the Consequence of Modernity, Cambridge Political Press Publishers, Cambridge.

easier to deal with this recent issue. [272] Working together brings in new idea and new methods of approaching matters related to cybercrime. [273]

The one challenge that Kenya faces is over-regulation.[274] It has much legislation that cover matters related to cybercrime, but these laws do not harmonize with the rest of the laws. There is no order as to which law will supplement the other and which one will supersede the other one in case of conflict.[275] There are other legislations like the data draft bill which has not been passed but have sentimental value in matters relating to cybercrime. These legislations make it hard to fight cybercrime. There is need to harmonize such laws so that they can co-exist with the already present laws.

The existing laws have established a territorial jurisdiction.[276] It has provided for the conditions under which the courts of Kenya are granted jurisdiction to hear the matter. It has missed the vital apart that entails attack launched from third party country.[277] Jurisdiction principle concerns itself with the attacks that are launched from a certain country without looking at the attacks that may be launched via an unknowing country. [278]For the laws of the laws to totally cover the essentials parts of cybercrime,[279] there are need to amend the main act that relate to the nature of cybercrime, such as the evidence act.[280] The fact that the act recognizes the existence of electronic evidence is not enough. There is need to amend such acts in order to have a comprehensive legislation.[281]

4.5.4 Ghana

Ghana has to deal with the rising issues of cybercrime in that it has developed from simple fraud where they used to sell fake products to online scamming.[282] Ghana legislative body has

[272] Sussman Ma, (1999), the Critical Challenges from the International High- Tech and Computer related Crime at the Millennium, 9, Durke Journal of Comparative and International law, Europe.
[273] Giannis Stamatellos, (2007) computer ethics a global perspective, Jonas and Bartlet Journal, Athens.
[274] Peterson Obara et al, 2011, Effects of Cybercrime on State Security: Types, Impacts and Mitigating with the Fiber Optic Development in Kenya, 20(11), Journal of Assurance and Cyber Security, Kenya.
[275] Souter David & Kerretts-Makau, (2012), Internet Governance in Kenya: An Assessment for the Internet Society, ICT Development Associates Ltd, Kenya.
[276] Zavier Geese, (1998), the State of Law on the Cyber Jurisdiction on the Internet,1, Journal of International Law California Pacific School of Law.
[277] Laudon Kenneth and Traver Guercio, (2011) E- commerce 13th Edition Pearson Education Ltd, Columbia.
[278] Yar Majid, (2006), Cybercrime and Society, Sage Publications Ltd, India.
[279] Nasi Ali, (2004), Legal Issues involved in E- commerce, Journal of Information and Technology, Vietnam.
[280] Murungi M M, (2011), Cyber Law in Kenya, Kluwer law and business International Journal, Kenya. 145
[281] Nykodym Nick and et al, (2004), The Worlds Current Legislative Efforts against Cybercrime, 20(5), Journal of Computer Law and Security, Ohio.
[282] Danquash Lounge et al, (2011), An Empirical Test of the Space Transition of cyber criminality: The Case of Ghana and Beyond, 4(2), African Journal of Computing and Cyber Criminality, Ghana.

concentrated more on financial frauds unlike the other aspect of cybercrime. E-commerce is a worldwide trading activity that involves different e-commerce aspects.[283] It has overlooked the aspect of cybercrime. From the above discussion it can be said that the legislation is not comprehensive enough to address the matter facing the state. [284]An example is the issue of jurisdiction which basses itself on the financial fraud. These provisions are limited in that it does not cover the entirety of cybercrime.[285]

4.6 Conclusion

From the above discussion it can be said that the United Kingdom and South Africa have developed legislations that has curbed cybercrime from different perspective. They have adopted other measures in addition to the existing laws that ensure that they have protected their country from the adverse effect of cybercrime. Kenya as a state can adopt certain measures that are cost effective in order to deal with cybercrime. There is need to amend the existing law to cover the present and future issues that may arise as the South African government have done.

[283] Boateng Richard et al, (2010) "Cyber Crime and Criminality in Ghana: Its Forms and Implications", Americas Conference on Information Systems (AMCIS) 2010 Proceedings, Ghana.
[284] Agyeman Frank and Asirifi Michael, (2015), The Impact of Cyber Crime on the Development of Electronic Business in Ghana,4(1), European Journal of Business and Social Science, Ghana.
[285] Smith Daniel, (2008), A Culture of Corruption: Everyday Deception and Popular Discontent in Nigeria Princeton, Princeton university press, Nigeria.

CHAPTER 5

5.0 RECOMMEDATAION AND CONCLUSION

5.1 Recommendation

Kenya is considered a developing country that is trying hard to attain the best standard of digitization in its economic sphere. Kenya has tried within its capacity to deal with cybercrime.[286]From the discussion contained in chapter three and four we can say that Kenya has so much to do in terms of coming up with measures and ensuring such measures are able to curb cyber related crimes. Some of the recommendations that should be enforced include:

5.1.1 Effective data protection bill

Kenya has come up with laws and legislations to ensure that cybercrimes do not prevail. With such legislation in place various challenges have come up making the enforcement of such legislations difficult. Among other legislations that fall within this bracket includes the data protection bill which has been proposed but not yet adopted by the Kenya government. The bill has one of the best propositions as it tries to complement the existing laws.[287] This is an essential feature when it comes to e-marketing. The easy access of information can be said to have affected e-marketing and since there are inadequate legislation to protect the privacy of e-marketing transaction then it may not thrive as well as it should.[288] Data protection is a critical part of e-marketing. There is need to develop a law that ensure that he information that is passed through the internet is secure.[289] This goes hand in hand with the issues of logs and register. There are many cybercafés and Wi-Fi hotspots in Kenya, most individual opt to use such spots based on the fact that they will have free access to the internet. The proposed data protection bill should entail the procedure of securing the logs on all computers and how they can be preserved in order to be used in cases of emergencies.

5.1.2 Amendment of Section 106 of the Evidence Act

[286] Milis Koen Mercken,Roger (2002). Success factors regarding the implementation of ICT investment projects,80(1), International Journal of Production Economics, Hasselt University.
[287] Murungi Michel, (2011), Cyber law in Kenya, Kluwer Law International Journal, Kenya.
[288] Mansell Robin, (2003), Electronic Commerce: Conceptual Pitfalls and Practical Realities. Prometheus Publishers, United Kingdom.
[289] David Souter and Monica Kerretts-Makau, (2012), Internet governance in Kenya: An Assessment for the Internet Society, International Law Journal, Kenya.

This section provides for the standard set for the admissibility of electronic evidence. The court in interpreting this section has come up with different meanings. Initially, this was only applicable to criminal cases. Overtime civil and commercial cases started relying on this section in order to achieve justice.[290] The constitution of Kenya provides that everyone has a right to fair hearing.[291] The section provides that for any electronic evidence to be admitted in a court of law, there is need for one to provide a certificate stating that the computer containing the evidence is authentic and is functioning properly. This article minimizes the admissibility of such evidence. This part limits itself to authentic computer. E-marketing allows one to use any device he so wishes to conduct with business. [292]At the time of transaction individuals don't usually look at the type of device they are using. This section should be amended in order to include all types of computer generated evidence.

5.1.3Sentencing of Computer Related Crimes

The penalties that are provided for within the legislation for anyone who commits a cybercrime have a minimum of three years imprisonment which is not enough.[293] The offender is pretty much sure that, once he has served this sentence then he will go back to normal and enjoy their benefits. [294] Penalties placed ought to deter anyone from committing any cybercrime.[295] For this to work comprehensively, apart from the years stipulated, the legislation should place provision that will compel the offender to surrender all the returns that he obtained when committing the crime.

5.1.5 Need to Train the Judicial Officers.

Cyber related crimes is a complicated matter and this has been seen from the admissibility of evidence.[296] Kenya does not have any forensic lab that can be used to process data which contains the evidence required. Establishment of such labs will enable one to preserve the evidence obtained that would otherwise be destroyed or lost.

---

[290] Zeinab Karake and Lubna Qasim, (2010), Cyber law and cyber security in Developing and Emerging Economies, Edward Elgan publishing, University of Maryland.
[291] Article 51 of the Constitution of Kenya.
[292] Smyth Thomas et al, (2010), Deliberate interactions: Characterizing Technology use in Nairobi, Kenya, In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems ACM, Kenya.
[293] Lillian Edwards and Charlotte Waelde, (2009), Law and the internet, 3rd edition, Hart publishing, Oxford and Portland.
[294] Bell Reve. (2002), The prosecution of computer crime, 9(4), Journal of financial crime, USA.
[295] Bell, R. E. (2002). The prosecution of computer crime. Journal of financial crime, 9(4), USA.
[296] Goel Ritendra, (2009), E-commerce, New age international Pvt Ltd publishers, South India.

In addition to that there is need to train all the individuals who are going to participate in cybercrime issues.[297] The government should implement a law that will state the responsibility and the function bestowed upon such officers. Such training will equip the investigators with both legal and technical requirements to approach cybercrime.[298] The training may also involve other expertise from other well-developed country. [299]

5.1.6 Online Payment and Mobile Money[300]

Online payment is the only method that is used in online transactions.[301] As seen the laws of Kenya are inadequate in that they do not entail the nature of e-commerce.[302] An individual may order goods that are not located within the jurisdiction of the country. The main question is what laws will be applicable in case of a conflict?

The laws that exist are inadequate since they do not offer full protection of consumers. There is need to implement policies and procedure that are used to address such matters. The National Payment Service Act that govern such. Credit cards were majorly used to carry out payment, now this has evolved to digital currency such as bitcoin an crypto currency.[303] The new way of payment has created a vacuum that allows money laundering to take place. There is need to endure a secure banking system to allow consumers to buy goods.[304]

Mobile transaction is a new emergence within e-commerce market.[305] Most merchants and consumers use the phone in order to carry out e-commerce activities.[306] Mobile money is the mode

[297]Marcelline Fusilier and Penrod Charlie, (2013), E-Business Curricula and Cybercrime: A Continuing Error of Omission?1(2), Universal Journal of Educational Research, Northwestern State University of Louisiana, Louisiana.
[298] Marcelline Fusilier and Penrod Charlie, (2009), E-crime prevention: An investigation of the preparation of e-commerce professionals, 8(1), Journal of Internet Commerce, University of West Florida.
[299] McCrohan Kevin et al, (2010) Influence of awareness and training on cyber security, 9(1), Journal of In Bakar AbuCyber Law Policies and Challenges, Butterworth's Asia, Kuala Lumpur.
[300] Dr. Kenneth Wanjua et al, (2012), factors affecting adoption of Electronic Commerce by Small Medium Enterprises in Kenya, Business Journal Kenya.
[301] Diane Mullenex and Anne-Sophie Mouren, (2012), M-payment in Africa: Great Means to Great Ends, Regulatory Communications Journal, Germany.
[302] Gheysari Hamed et al, (2012), E-commerce Reality and Controversial Issue, 2(4), International Journal of Fundamental Psychology & Social Sciences, United Kingdom.
[303] Claessens Joris et al, (2002), On the security of today's online electronic banking systems, 21(3), Computers and Security Journal, Malawi.
[304] Liao Zhang and Cheung M.T, (2002), Internet-based E-banking and Consumer Attitudes: an empirical study. Information & Management, Japan.
[305] Otieno Erick and Kahonge, Andrew, (2014), Adoption of Mobile Payments in Kenyan Businesses: A case study of Small and Medium Enterprises (SME) in Kenya, 107(7), International Journal of Computer Applications, Kenya.
[306] Hutchinson Damien and Warren Matthew, (2003), Security for Internet Banking: A Framework, 16(1), Logistics Information Management Journal, Australia.

of payment that has infiltrated the market.[307] The state may be needed to make laws that ensure the efficiency of such transaction. The CBK promulgate the Money Remittance Regulation, 2013, that was used to regulate corporate banking.[308] The downside of this regulation is that it does not include anything related to mobile banking.[309]

5.1.7 Harmonization of the Laws

There is need to harmonize the existing laws in order to deal with matters related to e-commerce. Kenya has implemented so many laws which brings issues as to what law will be applied and which law supersedes which one. This has made it hard to implement such laws.

5.1.8 Amendment of the Penal Code

Section 264 of the penal code entails what can be stolen. It provides that:

"Every inanimate thing, which is the property of any person, and which is movable is capable of being stolen"

This section does not include data information that can be obtained from hacking or other criminal means. E-marketing involves the exchange of information. Such information can be obtained without authorization.[310] They should make an addition on this section so as to include information as a thing that can be stolen.

5.1.9Electronic Signatures

The laws have stipulated that signatures are mandatory in order to ensure that the integrity of e-commerce transaction is protected. This is a big step in controlling the e-transaction. The electronic signatures are based on the transaction of the customer and bank. This type transaction demand that the replacement of personal information between man and the machine, thus there is need to

[307] Peterson Obara Magutu et al (2011), E-commerce Products and Services in the Banking Industry: The Adoption and Usage in Commercial Banks in Kenya, Ibima Publishing Journal of E- banking Systems, Kenya.
[308] Regulation 4 Money Remittance Regulation, 2013.
[309] Andiva Barnabas, (2015), 'Mobile Financial Services & Regulations in Kenya, Competition Authority of Kenya Journal, Kenya.
[310] Almeida Alberto, et al, (2007), Promoting E-Commerce in Developing Countries Internet Governance and Policy, International Governance Journal, Paris.

ensure clarification of such.[311] In addition to ensure such integrity is upheld, the government may implement the following measures:[312]

- ✓ Ensure that merchants have a way of identifying their customers
- ✓ E-identification of e-commerce can be done through the national identity cards which will be required to during the e-transactions. This reduces cyber fraud[313]

5.1.10Conclusion

The research set up was based on the impact of technological advancements on trade in relation to the law. It majorly focuses on how the merchants incur losses due to such practice. This aspect has provided an in depth understanding on how Kenya has tried to implement laws to deal with such issues. The legislations that are placed within the state have proven inadequate based in the datum that they do not cover the entirety of cyber related crimes. Kenya as a state has acknowledged the existence of cybercrime that is why it has placed other bodies to help in curbing such vice within the state. The research has also focused on other legislation of other countries and how they have addressed matters relating cybercrime. From such studies it can be said that e-marketing regulation is a collective responsibility among different people. Co-operation is an important piece in dealing with cybercrime. International co-operation is advised to address matters of extraterritorial border. [314]The laws implemented should apply to a state that is a party to the agreement.

Creating of awareness and consumer protection is one of the measures that can be taken to ensure that cybercrime does not have adverse effect in e-commerce.[315] The protection consumers can be promoted if Kenya creates a different platform that can be used to address cybercrime. This platform should not only be adopted by Kenya alone but other developing countries should come together to set up an organization that will be used as a platform. It will be time saving and financially effective as they will deal with consumers from different countries.

---

[311] Vanhoose David, (2011), E-commerce economics, second Edition, Routledge Publishers, United Kingdom.
[312] Lewis Andrew and Baker Stewart, (2013), The economic impact of cybercrime and cyber espionage, Center for Strategic and International Studies Journal, Washington, DC.
[313] Smedinghoff Thomas, (2008), The Legal Challenges of Implementing Electronic Transactions, Uniform Commercial Code Law Journal, Chicago.
[314] Zittrain Jonathan, (2005), Internet Law Series: Jurisdiction, Foundation Press, New York.
[315]Hua Huang and Yang Cai, (1995), Organization and Management Innovation: Under the Context of E-Business, 20(3), Journal of Information Management and Information Systems, Fudan University, Shanghai.

5.2 BIBLIOGRAPHY

5.2.1 BOOKS

Cheeseman Henry, (2001), 'Business Law: Ethical, International and E-commerce Environment', 4th Edition, Prentice-Hall Publishers, USA.

Avtar Singh, (2006).Principle of Mercantile Law, 8th Edition, Eastern Book Company, India.

Prashant Mali, (2010), 'Cybercrime and Penalties', First Edition, Snow White Publications, India.

Simon Allan & Shaffer Steven (2001), 'Data warehousing and Business Intelligence for E-commerce: Blending E-commerce Theory and Application', IEEE Computer Society Publishers, United States of America.

Michel M. Murungi, (2011),'Cyber law in Kenya', Kluwer Law International 2011, Kenya.

Kshetri N, (2010) 'Global Cybercrime Industry, Economic, Institutional and Strategic Perspectives', second Edition, Springer, United State of America.

Gottschalk Petter, (2013).Policing cybercrime. First Edition, Ventus publishing Aps, Denmark.

Justice Yatindra Singh, (2012) "Cyber Laws", Fifth Edition, Universal Law Publishing Company Pvt Ltd, New Delhi – India.

SChmalleger Frank and Pittaro Michae, (2008), 'Crimes of the Internet: Routine Activity Theory', 1st Edition, Prentice-Hall Press Upper Saddle, United State of America.

Newman Graeme and R.V Clarke, (2003) Superhighway Robbery: Preventing E-commerce Crime, 1st Edition, Willan Publishers, United Kingdom.

Durkhein Emile, (1993). "Ethics and the Sociology of Morals", 2nd Edition, Macmillan Company, New York.

Feslon Marcus and Boba Rachel, (2010), 'Crime and Everyday Life: Sociology Criminology', 5th Edition, SAGE Publications Inc. Texas State University, United States of America.

5.2.2 JOURNALS

Kyobe Michael,(2008), 'The Influence of Strategy-making Types on IT Alignment in SMEs', 10(1), Journal of System and Information Technology, United States.

Enrico Calandro et al, (2012), "Internet Going Mobile: Internet Access and Usage in 11 African Countries," Journal of Research ICT Africa, 2012, Sub Saharan.

McCrohan Kevin, (2003).'Facing the threats to Electronic Commerce', 18(2), Journal of Business & Industrial Marketing, George Mason University.

Demombynes Gabriel and Thegeya Aaron, (2012), "Kenya's Mobile Revolution and the Promise of Mobile Savings, Journal of Policy Research work, Kenya.

Orinobi Tokunbo, (2013), 'The Growth of E-commerce in Nigeria' Legal and Institutional Framework of E-commerce in Nigeria International Journal of Business and Social Science, Nigeria.

5.2.3 REPORTS

WTO, e-commerce in developing countries opportunities and challenges for small and medium-sized Enterprises [2013]