Strathmore University
Law School

The impact of cybercrime on e-commerce and regulation in Kenya, South Africa and the United Kingdom

Sinesipho Ralarala

Submitted in partial fulfilment of the requirements of the Master of Laws degree, School of Law, Strathmore University.

Strathmore Law School
Strathmore University
Nairobi, Kenya

June 2020

DECLARATION

I declare that this work has not been previously submitted and approved for the award of a degree by this or any other University. To the best of my knowledge and belief, the thesis contains no material previously published or written by another person except where due reference is made in the thesis itself.

Sinesipho Ralarala

…….....

…….....

APPROVAL

The thesis/dissertation of **Sinesipho Ralarala** was reviewed and approved by the following:

Dr Isaac Rutenburg
Senior Lecturer, Strathmore Law School,
Strathmore University

Professor Francisco B Lopez-Jurado
Dean, Strathmore Law School,
Strathmore University

Dr Bernard Shibwabo
Director, Office of Graduate Studies,
Strathmore University

ACKNOWLEDGEMENTS

I would like to extend my gratitude to my parents, family, and friends for showing me unwavering support and believing in me even in moments when I did not believe in myself. I am also indebted to my colleagues and supervisor, Dr Isaac Rutenburg, for his helpful comments and guidance throughout this research exercise.

LIST OF ABBREVIATIONS

AST	Adaptive Structuration Theory
BAKE	Bloggers of Kenya Association
B2B	Business-to-business
B2C	Business-to-consumer or business-to-customer
CPNI	Centre for the Protection of National Infrastructure
CSIRT	Computer Security Incident Response Team
C2B	Consumer-to-business
C2C	Consumer-to-consumer
CREST	Council for Registered Ethical Security Testers
CLRNN	Criminal Law Reform Now Network
NIS Directive	Directive on Security of Network and Information Systems
GDP	Gross National Product
ICT	Information Communications Technology
IT	Information technology
IACP	International Association of Cyber-crime Prevention
LDCs	Least Developed Countries
NCFP	National Cybersecurity Policy Framework
OECD	Organisation for Economic Cooperation and Development
TAM	Technology Acceptance Theory
SDF	Secure Domain Foundation
SABRIC	South African Banking Risk Information Centre
SABC	South African Broadcasting Corporation
SALC	South African Law Commission
UK	United Kingdom

LIST OF STATUTES AND INTERNATIONAL INSTRUMENTS

International Instruments

African Union Convention on Cybersecurity and Personal Data Protection

Council of European Union Convention on Cybercrime

General Data Protection Regulation

Kenya

Computer Misuse and Cybercrimes Act 5 of 2018

Data Protection Act 24 of 2019

Kenya Communications Amendment Act 2008

Kenya Criminal Procedure Code Cap 75

Kenya Information and Communications Act 2 of 1998

The Prevention of Terrorism Act 30 of 2012

South Africa

Cybercrimes and Cybersecurity Bill 2017

Electronic Communications and Transactions Act 25 of 2002

Prevention of Organised Crime Act 38 of 1999

Protection of Personal Information Act 4 of 2013

Regulation of Interceptions and Provision of Communications-Related Information Act 70 of 2002

United Kingdom

Civil Contingencies Act of 2004

Communications Act of 2003

Computer Misuse Act of 1990

Data Protection Act of 2018

ABSTRACT

As the use of the internet increases across the world, it becomes imperative to be aware of the ways in which economies can benefit from such use and to be equally aware of the impediments to the maximisation of these benefits. Cybercriminal activity is considered to be one of the impediments to the economic growth promised by e-commerce. This study seeks to examine the impact of cybercrime on e-commerce and regulation, a research direction that has potential to provide insight in respect of the mechanisms meant to safeguard against cybercrime. The study underscores the need to direct more robust efforts towards combating cybercrime in both Kenya and South Africa, an idea that could lead to significant contribution to the growth of African economies (namely Africa).

This study is mainly underpinned by the *Routine Activity Theory*. A descriptive research design is employed. The study relies on reviews of relevant documents which include but are not limited to: legislation, case law, international law instruments. With these materials, an analysis has been carried out to interrogate cybercrime and cybersecurity and the way in which these concepts relate to each other in the context of e-commerce, and the extent to which they impact e-commerce and regulation.

The findings reveal that while Africa is ahead of the international landscape in developing legislation, there are efficient mechanisms used internationally that African (mainly in Kenya and South Africa) dispensations can apply to her context. Future studies on this topic could broaden the scope of the study by exploring the impact of cybercriminal activity on Small Medium Enterprises which have also been identified as significant contributors to African economies.

Key words: cybercrime, regulation and e-commerce

TABLE OF CONTENTS

Chapter One: Introduction

1.1 Background to the Research

Upon the commercialisation of the internet and the rise in users seeking to participate in the World Wide Web in the 1990s, the term e-commerce was coined.[1] Electronic Commerce, which is more commonly known as e-commerce, embodies technologies and infrastructures.[2] E-commerce unites narrow applications, entire industries, the exchange of digitally encoded information and economic activity on the global marketplace known as the internet.[3] However, defining e-commerce universally is challenging because the internet and its e-commerce participants are various and complexly related. Moreover, the intricate relationships between all participants and technologies evolve rapidly.

This research makes use of the definition submitted by Cudjoe[4] which provides that e-commerce is: business, society, technology and skills selling and buying products as well as services. This, according to Cudjoe, is done with the aid of computers and the internet or handheld devices. The process entails ordering of services or products to the time of delivery to the customer or consumer. [5]

There are several types of e-commerce that have been identified and it is important to highlight which types are most relevant to this research:

- **Business-to-business (B2B)** e-commerce relates to a commercial activity between businesses, such as transactions that may take place between a retailer and a wholesaler.
- **Business-to-consumer or business-to-customer (B2C)** e-commerce describes the conduct of a business serving the end consumer with a product and/or service. Online banking and online retail are examples of this type of e-commerce.

---

[1] Cudjoe D, 'Electronic Commerce: State-Of-The-Art' 4(4) *American Journal of Intelligent Systems*, 2014, 136.
[2] Mann CL, Eckert SE and Cleeland Knight S, *Global Electronic Commerce,* Institute for International Economics, Washington DC, 2000, 9.
[3] Mann CL et al, *Global Electronic Commerce*, 9.
[4] Cudjoe D, 'Electronic Commerce: State-Of-The-Art', 136.
[5] Nemat R, 'Taking a look at different types of ecommerce' (1)2 *World Applied Programming*, 2011, 101.

- **Consumer-to-consumer (C2C)** e-commerce is commercial activity that involves transactions between consumers facilitated by a third party such as online auctions where one consumer sells, the other bids and the third party charges a fee for facilitating the sale.
- **Consumer-to-business (C2B)** e-commerce is a model where individual consumers are paid by companies for offering goods and services to companies.[6] These types of companies are those that operate largely online, such as Amazon.

Generally, the use of the internet has advanced human life quality. This is evident because the use of the internet in e-commerce is seen as an opportunity for developing countries and developing economies to gain more benefits from trade. On an e-commerce platform, the requirements to conduct business are less than in a traditional "brick and mortar" model using a physical building. For instance, there may be a requirement for storage space but one may still operate the business remotely meaning they would save on costs for rent when only paying for storage space. Therefore, a business might have fewer requirements for office infrastructure and maintenance, and thus, higher profit margins.[7] It can be said that the main benefit introduced by e-commerce is that it has enabled users to engage in international business, which is the term employed to describe any transaction of a commercial nature that crosses the borders of nations.[8]

There have been inadvertent consequences in the use of the internet in e-commerce[9] mostly in the form of cybercrimes. Therefore, in this dissertation, I have explored the legal and technological ways that can be employed to respond to these cybercrimes. In doing this more effectively, I have reviewed the cybercrime response mechanisms already in existence in three jurisidictions and submit recommendations as to how these can be improved. Central to this

[6] Nemat R, 'Taking a look at different types of ecommerce', 111 – 112.
[7] Cudjoe D, 'Electronic Commerce: State-Of-The-Art', 136.
[8] Wild JJ, Wild KL and Han JCY*, International Business: The challenges of globalization*, Pearson Education Inc., New Jersey, 2010, 32.
[9] Raghavan AR and Parthiban L, 'The effect of cybercrime on a Bank's finances' 2(2) *International Journal of Current Research and Academic Review,* 2014, 173.

dissertation is the Kenyan, South African and United Kingdom legal dispensations, as well as an outline of the jurisdictional issues that arise with respect to prosecution for these crimes.

Since there has been an increasing reliance on the internet by individuals and organisations, cybercrimes have posed financial threats along with theft of personal information and business data.[10] Information for a competitive purpose or that which is for political purposes has been identified as one of the main motivations behind cybercriminal activity; in addition to this, financial gain has proved to be another motivator for cybercriminals. Apart from these main motivators, fun, grudges, and ideologies also drive a number of cybercriminals.[11] There are different categories of cybercrimes that impact the types of e-commerce discussed above:

- **Phishing** (also known as spoofing) is an attempt to ruse consumers or customers into divulging security information that is personal (this may include bank account numbers or credit card information) by posing as trustworthy business accounts.[12]
- **Spam** mail which involves distributing bulk emails in order to advertise goods or services, usually at discounted prices, which may turn out to be fraudulent; and hacking, which has been defined as the unauthorised access into peoples' computer systems and the subsequent use of such systems. [13]
- **Hacking** takes place in a number of stages, from information gathering to scanning to finally entering into the target system (for instance a business' computer system). Thus, it has been identified as being similar to traditional robbery but that which occurs through the use of the internet.
- **Identity theft** entails the theft of personal and sensitive information about people and the use of that information to commit theft or fraud.[14]
- **Internet auction fraud** occurs where nonexistent goods/services are advertised and a consumer is hoaxed into paying for such 'goods/services.'

[10] Raghavan AR and Parthiban L, 'The effect of cybercrime on a Bank's finances', 173.
[11] https://www.vircom.com/blog/cybercriminals-who-they-are-and-why-they-do-it/
[12] Jahankhani H, Al-Nemrat A, Hosseinian-Far A, 'Cybercrime Classification and Characteristics' *ReseachGate,* 2014, 157, https://www.researchgate.net/publication/280488873 , on 10 March 2019.
[13] Jahankhani H, Al-Nemrat A, Hosseinian-Far A, 'Cybercrime Classification and Characteristics', 136.
[14] Jahankhani H, Al-Nemrat A, Hosseinian-Far A, 'Cybercrime Classification and Characteristics', 136.

The categories of cybercrime discussed above, find relevance to this study because when each is committed, there is an interference with the transactions between consumers and consumers, businesses and businesses, or consumers and businesses. Such interferences may also lead to mistrust between the actors in business activity.

From the above discussion, it can be deduced that cybercriminal activity has the effect of impeding the ability of users to engage safely in trade, which in turn has inopportune consequences to the economy. Put differently, since e-commerce is conducted on the internet and cybercrimes take place on the internet as well it can be said that these two activities are necessarily connected because the presence of one (cybercrime) affects the proper functioning of the other (e-commerce).

1.2 Problem Statement

The use of technology has become increasingly popular in our world. As has been alluded to above, e-commerce has brought benefits to trade, especially for countries such as Kenya and South Africa which are considered to be developing.

This dissertation posits that the lack of specialised regulatory and technological mechanisms to manage cybercrime has adversely impacted advancements in trade, especially for developing countries like Kenya and South Africa. Because of the increase in crimes (with an increase from 3.8 million to 10.2 million recorded in Kenya)[15] which breach the cybersecurity of internet users, and in particular those involved in different types of e-commerce, this malicious activity has impacted the law. Thus this calls for rigorous regulation to improve the effectiveness of existing legislation in Kenya, South Africa and the regulations that exist in United Kingdom which is a more developed jurisdiction.

This study is concerned with the categories of these crimes, which affect the types of e-commerce and have been discussed above. It is important to note that this issue is multi-

[15] Capital FM Kenya, 'Plight against cybercrime rife in Kenya' 02 July 2019 <https://www.capitalfm.co.ke/business/2019/07/plight-against-cybercrime-rife-in-kenya/> on 12 August 2019.

layered in that it exists on an international level, because of the multijurisdictional nature of the crimes committed. The possible solutions to the outlined issues may be found through the development of existing legislation in Kenya and South Africa and in the development of security mechanisms in information technology (IT).

1.3 Objectives of the Research

The research has been conducted with the broad objective of assessing what measures are lacking in the regulatory and IT environments to guard against cybercriminal activity as a factor that impedes the growth promised by e-commerce to economies.

1.4 Hypothesis

The proposed hypothesis for this research is stated as follows: the development of cybercrime and data privacy legislation in combination with the refinement of cybersecurity measures in IT is positively associated with mitigating cybercrime, which affects e-commerce transactions.

The specific impact of cybercrime that I investigate in this research is that of the ability of users to partake in e-commerce. The impact related to jurisdictional matters that arise when responding to cybercrime has also been explored.

The hypothesis submitted above is based on the understanding that robust regulation in combination with enhanced technological mechanisms will tighten cybersecurity, and thereby, reduce the rates of cybercriminal activity.

1.5 Research Questions

This research propounds that effecting improvements to the legal framework together with software technology will result in advanced cybersecurity measures and, in turn, protect users from the rising cybercrimes. In light of this, a number of questions become relevant, with the primary question being:

1. What is the impact of cybercrime on e-commerce and regulatory frameworks in Kenya, South Africa, and the United Kingdom?

Secondary questions are as follows:

1. What constitutes e-commerce in Kenya, South Africa, and the United Kingdom?
2. What constitutes cybercrime in Kenya, South Africa, and the United Kingdom?
3. How does cybercrime impact regulatory frameworks?
4. What methods are employed in law and information communications technology to respond to cybercrime in Kenya, South Africa, and the United Kingdom?

1.6 Literature Review

As alluded to in the background to the problem, an unintended consequence that follows when users engage in e-commerce is cybercrime. The crime committed through the use of computers has resulted in financial damage amounting to billions.[16] Because companies do not always disclose all information on the impact of cyberattacks, it has proved difficult to accurately quantify the losses that are experienced by victims of cyberattacks. In spite of this difficulty, the results indicate that cyberattacks negatively impact businesses by disrupting them, causing loss of information, revenue, and damage to equipment. [17]

Developing technological and suitable legislation has been conceded to respond to cybercrime as well as to promoting cybersecurity, which are integral aspects in addressing this matter.[18] Insufficient protection measures pose a greater risk in developing countries because of the weaker safeguards and protection in these countries. Poor internet security may result in developing countries encountering challenges in promoting participation in e-commerce.[19]

[16] Podgor ES, 'Cybercrime', 99.
[17] Bendovschi A, Cyberattacks – Trends, Patterns and Security Countermeasures, International Conference on Financial Criminology organisd by Wadham College, Oxford, 13-14 April 2015, 28-29.
[18] Gercke M, 'Understanding Cybercrime: phenomena, challenges and legal response' *International Telecommunications Union*, 2012, 97 <https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014_E.pdf> on 27 April 2019.
[19] Gercke M, 'Understanding Cybercrime: phenomena, challenges and legal response' *International Telecommunications Union*, 2012, 4.

On the African continent, it has been submitted that cybercrime has cost Africa's economy billions, with e-commerce costing the continent an estimated 173 million USD owing to its vulnerability to cybercrime.[20]

Serianu, a Pan-African consulting firm, committed to providing consulting services on technology, has shed much light on the progression of cybercrime and cybersecurity in Kenya (and other African countries) over the past seven years. In 2012, it was reported that Kenya's percentage for cybercrime is significantly higher than what has been recorded on a global scale.[21] The firm, in 2013, noted that the relationship between internet usage and cybercriminal activity was such that as the former increases, so does the latter. Furthermore, it was recorded that the malware activity increased from what was recorded during the previous year.[22] In 2016, it was submitted that the approximate expenditure on cybercrime amounts to 175 million USD in Kenya,[23] this estimation went up to 210 million USD in 2017.[24] An approximation of certified professionals in the IT space was also recorded in these reports. The number of professionals has proved to be wanting as there are seemingly not enough professionals with the skill set to assist in combating these issues.

In South Africa, cases of cyber-espionage, data exposures of a malicious nature, and hacking have been recorded to have taken place between the years 2013 to 2017. These attacks are reported to have cost the country millions of ZAR. The South African Banking Risk Information Centre (SABRIC) submitted that cyberattacks cost the country an estimation of 157 million USD annually. [25] Toure, who was previously the secretary of the International Telecommunications Union, stated that cybercriminals deem the African continent as an ideal place to conduct illicit activity with impunity. [26]

---

[20] Dahir AL, 'Cybercrime is costing Africa's businesses billions' *Quartz Africa*, 2018 <https://qz.com/africa/1303532/cybercrime-costs-businesses-in-kenya-south-africa-nigeria-billions/ > 05 September 2019.
[21] Serianu, *Kenya Cybersecurity Report,* 2012, 5.
[22] Serianu, 2013, 13.
[23] Serianu, 2016, 10.
[24] Serianu, 2017, 11.
[25] Van Niekerk B, 'An Analysis of Cyber-Incidents in South Africa' 20 *The African Journal of Information and Communication,* 2017, 117 – 118.
[26] Kshetri N, 'Cybercrime and Cybersecurity in Africa' 22(2) *Journal of Global Information Technology Management*, 2019, 77.

I argue that this statement highlights the importance of the creation of punitive sanctions for such illegal activity as a means to deter such activity.

Several security technologies have, over the years, been developed worldwide in an effort to maintain secure networks.[27] Such technologies are Intrusion Detection Systems, Pretty Good Privacy, Secure Socket Layer, IP Security, and Wired Equivalent Privacy, to name a few. Cybercrimes continue to rise in spite of these developments.[28]

Internal and external security countermeasures have been developed in response to the need for cybersecurity to protect users against cybercrimes. The internal countermeasures that have been submitted are continuous risk assessment, maintenance of a healthy IT environment, authentication; internal commitment and responsibility, access to information, data retention, and independent reviews. Where external countermeasures are concerned, there are various nonprofit organisations that have attempted to make users aware of the risks of and exposure to cyberattacks as well as how users can defend themselves from such attacks. Among these organisations are the Secure Domain Foundation (SDF) and the International Association of Cyber-crime Prevention (IACP). In addition to these organisations, Google has developed a team – Project Zero – which seeks to analyse vulnerabilities in other company codes and their own in order to improve software products and ultimately reduce the risk of cyberattacks. Financial institutions such as AXA Corporate Solutions Company have introduced insurance products that cover the costs lost as a result of a cyberattack.[29]

In addition to this, other external measures to promote cybersecurity are the developments to legislative frameworks in response to cybercrime and to promote cybersecurity by deterring cybercriminals. The *Computer Misuse and Cybercrimes Act* was promulgated in May of 2018 in Kenya. This piece of legislation mainly purports to ensure that using computer systems for illegal purposes is prevented, also to protect the confidentiality of users and data. The offences,

[27] Comer DE, *Computer and Networks Internets with Internet Application,* Pearson Education Inc., New Jersey, 2004, 618 – 619.
[28] Comer DE, *Computer and Networks Internets with Internet Application,* 618 – 619.
[29] Bendovschi A, Cyberattacks – Trends, Patterns and Security Countermeasures, 28-29.

investigation procedures, and international co-operation, among other provisions, are outlined in the Act. Until now, no case law has been reported where the above-mentioned Act has been applied. However, the statistics of cybercrime and their impact are indicative of the need that arose for the development of legislation to address these crimes. In a 2016 report, it was noted that at least 19 organisations in Kenya were affected by a ransomware virus that was ongoing globally.[30]

In South Africa, the *Regulation of Interceptions and Provision of Communications-Related Information Act* (*RICA*),[31] and the *Electronic Communications and Transactions Act* (*ECT*A)[32] are the main regulations that seek to address cybercrime. It is in this latter Act, that the jurisdiction for cybercrimes is outlined.[33] There are other pieces of legislation enacted prior to the Acts mentioned such as the *Prevention of Organised Crime Act.*[34] The most recent development in the South African legal dispensation is the *Cybercrimes and Cybersecurity Bill*, which was proposed to address the shortcomings and gaps that have been found in prior pieces of legislation.[35]

The United Kingdom has been far ahead of the two jurisdictions mentioned above with its *Computer Misuse Act* that was enacted in the nineties.[36] Over a decade later the *Data Protection Act* came into force in 2018.[37]

Because of the cross-border nature of international business activity,[38] the crimes committed in this field may give rise to issues of jurisdiction.[39] The matter of jurisdiction is relevant to this research because one of the solutions proposed is the development of legal frameworks

[30] Nida T, 'The Impact of Cyberattacks on Financial Institutions' 23(2) *Journal of Internet Banking and Commerce*, 2018, 7.
[31] *Regulation of Interception of Communications* (Act No. 70 of 2002).
[32] Section 85 – 89, *Electronic Communications and Transactions Act* (Act No. 25 of 2002).
[33] Section 90, *Electronic Communications and Transactions Act* (Act No. 25 of 2002).
[34] *Prevention of Organised Crime Act*(Act No. 38 of1999)
[35] Schultz CB, 'Cybercrime: An Analysis of Current Legislation in South Africa' unpublished, University of Pretoria, Pretoria, 2016, 9.
[36] *Computer Misuse* (Act of 1990).
[37] *Data Protection* (Act of 2018).
[38] Wild JJ et al, *International Business*, 32.
[39] Podgor ES, 'Cybercrime: National, Transnational or International' 50(97) *The Wayne Law Review*, 2004: 97.

that respond adequately to cybercrime and in order to have an adequate response jurisdiction must be provided for. Jurisdictional issues may arise because of differences in the definition of the crime and the subsequent penalties imposed for that defined crime in a specific state.[40] As a result, it becomes difficult to conduct investigations because procedural laws are specific to the territory in which they exist.[41] As early as 1980, the Organisation for Economic Cooperation and Development (OECD) issued Guidelines Governing the Protection of Privacy and Trans-border Flows of Personal Data, which encompassed guidelines and principles. In 2007, the OECD then published Cross-border Cooperation in the Enforcement of Laws Protecting Privacy. Data privacy is inadvertently connected to issues that relate to cybercrime because when categories of data, such as the private details of an individual, are easily accessible, it creates an environment that enables cybercriminal activity. There are universal principles that are applicable to data privacy, which are derived from these international instruments. Briefly, these principles may be stated as follows:[42]

- The processing of data must be done fairly and lawfully.
- When data is processed, the purpose for such processing must be fair and lawful and this processing should be done for a limited range of purposes.
- The nature of the data must at all times be accurate and if it is necessary to do so, the data must be updated at regular intervals.
- Where data is kept, it must be for limited and not unnecessarily prolonged periods.
- The rights of the data subject must be taken into account when data is processed. The data must not be processed in a manner that infringes on such rights.
- The data should at all times be secure.
- Before data is transferred between nations, it must be ensured that there is adequate protection of the personal data

[40] Podgor ES, 'Cybercrime', 97.
[41] Brenner SW, Schwerha JJ, 'Introduction—Cybercrime: A Note on International Issues' 6(2) *Information Systems Frontiers*, 2004, 111.
[42] Mwangi RW, 'Data Protection Principles and Cybercrime in Kenya' unpublished, Catholic University of Eastern Africa, Nairobi, 2010,

There have been other more recent developments that I have focused on in this study because the use of the internet is ever-changing meaning more recent frameworks are relevant as older frameworks can quickly become obsolete. These developments include the Council of Europe's introduction of the *Convention on Cybercrime*[43] which seeks to establish uniform standards for the response to cross-border cybercrimes. The African Union also adopted the African Union *Convention on Cybersecurity and Personal Data Protection*[44] in 2014 with the aim of addressing the jurisdictional challenges that arise on an African level. In addition to this, the European Union promulgated the *Global Data Protection Regulation*, which frames the protection of private and personal data as a fundamental right.[45] These pieces of legislation are important because they seek to establish uniformity among legislative frameworks and avoid the confusion caused by those that are difficult to apply because of major territorial differences.

An analysis of the literature suggests first that cybercrime is a rising concern; second that the alarming increase in cybercrime acts as an impediment to business activities especially in developing countries and lastly, that the matter should be addressed in order to counter the adverse consequences. This study posits that an ideal response to this issue is the interface of a specialised regulatory framework together with advancements in technology to promote cybersecurity.

1.7 Theoretical Framework

The purpose of a theoretical framework is to provide guidance to a research study as well as to highlight the variables that the study seeks to assess and to explore the relationship that exists between such variables.[46]

A few theories that are found in information systems are the *Technology Acceptance Theory*, (TAM) which models that a user's perception of technology is deterministic of the user's

[43] Article 22, *Council of Europe Convention on Cybercrime*, 23 November 2001, ETS 185.
[44] African Union Convention on Cybersecurity and Personal Data Protection, 27 June 2014.
[45] Mcdermott Y, 'Conceptualizing the right to data protection in an era of Big Data' *SAGE Journals*, 2017, 1.
[46] Obeng-Adjei A, 'Analysis of Cybercrime Activity: Perceptions from a South African Financial Bank' unpublished, University of the Witwaterstrand, Johannesburg, 2017, 19.

acceptance of that technology.[47] The *Stages Theory* consists of concepts for assimilating the way in which IT is absorbed into business organisations. The *Structuration Model* describes the way in which changes in technology influence organisational design. Specifically related to the structuration model, is the *Adaptive Structuration Theory*, (AST) which detects the influence of changes to organisations in two ways. First, the various structures, which are dispensed by the technological advances, and second, the structures that emerge as the use of technology increases.[48]

This particular study combines elements from IT as well as cybercriminal activity and law, which indicates that two theories are relevant to this study. However, the focus has been placed on one theory. This theory being the Adaptive Structuration Theory, which is relevant to the element of the study that relates to information systems because various structures and bodies have emerged for purposes of cybersecurity. Where the crime aspect of this study is concerned, use of the *Routine Activity Theory* mainly has been made. According to this theory, it is the structure of routine everyday activity that influences criminal opportunity.[49] Underpinning this theory is the notion that structural changes in routine activity patterns have the ability to influence the rates of crime by affecting the confluence of the three elements of predatory violations. These elements are motivated offenders, suitable targets as well as a lack of guardians to guard against crime. Yar[50] has posited that the absence of one of these three elements is enough to aid the prevention of a complete predatory crime that involves direct contact.

It can be said that the presence of the mentioned three elements in cybercrime elucidates the alarming increase in cybercrime. In other words, the conditions (outlined in the routine

[47] Halawi L, McCarthy R, 'Which Theory Applies: An Analysis of Information Systems Research' *Issues in Information Sysytems,* 7(2), 2006, 252.
[48] Halawi L, McCarthy R, 'Which Theory Applies: An Analysis of Information Systems Research' *Issues in Information Sysytems,* 7(2), 2006, 253.
[49] Yar M, 'The Novelty of Cybercrime: An Assessment in Light of the Routine Activity Theory' *European Journal of Criminology (2)4,* 2005, 412.
[50] Yar M, 'The Novelty of Cybercrime: An Assessment in Light of the Routine Activity Theory' *European Journal of Criminology (2)4,* 2005, 413.

activity theory) for cybercrime to flourish are ideal. In order for the rise in cybercrime to be countered, one of these conditions must be altered.

To apply this directly to this study, I identify the three elements in this study to be: cybercrime, e-commerce and regulation. The motivated offenders are the cybercriminals, the suitable condition is the e-commercial activity on the internet, and the lack of a guardian is the lack of a specialised framework. I opine that if this last aspect is altered by developing a legal framework will aid the prevention of a complete crime.

1.8 Research Methodology

The research methodology of a study furnishes a strategic plan of the way in which the research will be executed, which is a tool that encompasses the application of research design and procedures for collecting and analysing data.[51]

A research design has been defined by Kerlinger[52] as the structure that seeks to address research questions and manage variance. The design may be used to convey the way in which the crucial elements of the research collaborate in an attempt to respond to the questions that are central to the research.[53]

There are several types of research design that have been identified in research methods, these include an exploratory design, which is the type employed where the field of research is new, and there are few or no studies that have been made that can be referenced. Another, explanatory design/analytical, is most suitable for studies that seek to explore a new universe, which has not been studied before. Such research designs exist among a variety of other types.[54]

---

[51] Njogore EW, 'Effects Cybercrime Related Costs on Development of Financial Innovation Products and Services: A Case Study of NIC Bank of Kenya' Jomo Kenyatta University of Agriculture and Technology, Nairobi, 2017, 33.
[52] Penial BB, 'Research Design' *ResearchGate*, 2017, 1 < https://www.researchgate.net/publication/308262064_Research_Design> on 27 April 2019.
[53] Penial BB, 'Research Design' *ResearchGate*, 2017, 2.
[54] Akhtar I, 'Research in Social Science: Interdisciplinary Perspectives' *ResearchGate*, 2016, 73 – 74 < https://www.researchgate.net/publication/308915548_Research_Design> on 27 April 2018.

In this study, the descriptive research design has been utilised. The descriptive research design may also be referred to as statistical research which illustrates events which exist as such. Where pinpointing and acquiring information related to a particular issue is necessary, this type of design is most useful. This is because a descriptive design entails an observer describing social events in a current situation.[55]

The procedure involved in a descriptive study, in general, and in particular to this research, can be outlined as follows: the selection of an objective for the research, determination of the manner in which data will be collected, selection of sampling, the collection of real data, and the evaluation of the conclusion that has been reached from the collection of data.[56]

The nature of this study being that information related to an issue has been identified and collected, determines that the descriptive design research method is most appropriate. Uncovering information to present a possible solution to the pressing issue of cybercrime as it relates to e-commerce is the purpose of this research. The technique for data collection that I have be employed is the review of documents and records, namely legislation, case law and international law instruments. With this material, I have made an analysis of what cybercrime and cybersecurity are and the way in which these concepts relate to each other in the context of e-commerce. This information has then be used to draw a comparison between existing situations and legislative frameworks in Kenya and those in South African for an African perspective as well as those in the UK for an international perspective. These three jurisidictions are the scope of this study. However, I have submitted a commentary on jurisdictional issues that arise where legislating cybercrime is concerned.

1.9 Assumptions

The problem identified in this research is constructed based on the assumption that if no robust cybersecurity measures are adopted, there will be a further increase in the cybercrimes committed which will affect the potential growth of e-commerce. Inadvertently, this will affect

[55] Akhtar I, 'Research in Social Science: Interdisciplinary Perspectives' *ResearchGate,* 2016, 75.
[56] Penial BB, 'Research Design' *ResearchGate*, 2017, 2.

the economies of Kenya, South Africa and the UK, since it has already been suggested submitted that e-commerce provides a significant contribution to economies.

1.10 Chapter Breakdown

In exploring the topic, the mini-thesis is comprised of four chapters with the first as the introduction. The second gives insight into the development of and the current legal dispensation in Kenya and South Africa to respond to cybercrime and the institutions that have emerged for cybersecurity. In the third chapter, the position in the UK is outlined to provide a perspective outside of the African continent and then I proceed to make use of the UK perspective as a point of reference to compare it to the African continent. In the fourth and final chapter the conclusion and recommendation on these findings are provided.

Chapter Two: Regulatory and Institutional Developments in Kenya and South Africa (African Perspective)

2.1 Introduction

In the discussion in the preceding chapter, it has been highlighted that cybercrime is a critical issue, especially for the African continent where technology could be a key factor in advancing the social and economic landscape. The promise of development driven by technology can be seen in the surfacing of technology hubs in Africa that bring about the promise of entrepreneurship and innovation to the continent. Kenya and South Africa are locations to such hubs among other countries on the continent.[57]

However, this development is stifled by a number of issues such as cybercrime. Another of these issues being that the focus of the African continent is, and has been, centred around the eradication of illnesses such as HIV as well as poverty, delivery of basic services, a rise in unemployment, addressing corruption have led to cybercrime being tackled as a peripheral issue.[58]

In this chapter, I delve into the discussion pertaining to the legislative developments that have been made up until this point in Kenya as well as in South Africa. In addition to this, I note the institutions that have emerged as a measure to respond to cybercrime and in turn promote cybersecurity and provide commentary on how effective such developments have been. This study proposes that this development is threatened by the rise of cybercrime which can be seen in costs of cybercrime, especially to e-commerce, as outlined in the first chapter.

[57] De Beer J *et al,* 'A Framework for Assessing Technology Hubs In Africa' 6(2), *Journal Of Intellectual Property And Entertainment Law*, 2017, 239 – 240.

[58] Gumbi D, 'Understanding the threat of cybercrime: A comparative study of cybercrime and the ICT legislative frameworks of South Africa, Kenya, India, the United States and the United Kingdom' published, University of Cape Town, Cape Town, 2018, 11.

2.2 Contextual Issues Relating to Kenya and South Africa

As it has already been established, we have witnessed a rapid surge in utilisation of the internet globally. This increase has brought support to the development in the e-commerce industry globally through mainly introducing novel methods and ways of transacting as well as presenting the promise of economic development for Least Developed Countries (LDCs). Currently, the top six e-commerce sites in Africa have been identified as the Jumia group which is a Nigerian based company operating in 14 countries in Africa; Zando as the subsidiary of Jumia which was launched on South Africa in 2012; Takealot founded in 2002 in South Africa and Kilimall known as Kenya's largest online shopping mall, among others. It is worth noting that the use of MPESA (mobile money) in Kenya has made a significant contribution to e-commerce activity as it has provided a somewhat secure platform on which mobile transactions can take place thus encouraging online purchases.[59]

E-commercial activity is recognised as a platform with the potential to contribute to income generation through the facilitation of trade and in this way as having the ability to contribute to gross national product (GDP) as this is likely to foster export growth and the creation of employment opportunities. With the use of e-commerce a local business has access to a wider market when it penetrates the internet space. In developing countries, where women are often on the side line with respect to making a contribution to household income, e-commerce presents an opportunity for women to trade since it encourages entrepreneurship. Furthermore, the use of the internet to engage in e-commerce activities creates a demand for specialised skills required to navigate cyberspaces which in turn creates a demand for individuals to be educated on those skills. This is beneficial to institutions for higher learning as it broadens the courses that they can offer to potential students.[60]

As I have highlighted above, e-commerce itself has not penetrated the African economy to the same extent that it has penetrated other economies. Where it has penetrated the African economy there are a number of challenges that hinder the potential growth and development

[59] Maseko F, '6 sites driving eCommerce in Africa' 26 January 2019 <https://www.itnewsafrica.com/2019/01/6-sites-driving-ecommerce-in-africa/> on 03 February 2020.
[60] Ndonga D, 'E-Commerce in Africa: Challenges and Solutions' 5 *African Journal of Legal Studies*, 2012, 244 - 246.

that can be fostered by e-commerce. The term 'digital divide' has been coined and is understood to describe the disparities identified between Africa and the rest of the world where Information Communications Technology (ICT) is concerned. Much of this divide is attributed to lack of access and poor usability of ICT infrastructure resulting from poor knowledge about ICT and the infrastructure. The other aspect, which is most relevant to this study, concerns the threat of cybercrimes. A result of the alarming rise in cybercriminal activity has been Africans being reluctant to make use of the e-commerce platform for goods and services. While Africans may use online websites to view products and services, most still opt to make use of these goods/services in the traditional way. Therefore, it is argued that with the development of robust regulatory mechanisms, which respond to the lack of awareness with respect to ICT as well as frameworks that respond to and control cybercrimes such that Africa can realize the potential of e-commerce to contribute to overall economic growth.[61]

2.2.1 Kenya

Where the types of cybercrime are concerned, in 2012 Serianu reported that spamming was on the rise in Kenya and that although spam emails were generally harmless advertising, a new breed of spamming which contain viruses was discovered. Botnets, Trojans and worms have also been identified as a cyber threat to the country's networks.[62] The top cyber threats in 2013 were reported as follows: Insider Threats mainly by employees; VoIP (Voice over Internet Telephony) PBX fraud where hackers gained access to business PBX phone systems to generate profit from making calls to international numbers; Social Media Attacks which consisted of cyber-bullying, hate speech, posting of obscene images; Denial of Service attacks; Botnet Attacks; Cyber Espionage; Mobile Money Fraud and Online/Mobile Banking. The attacks and threats of this nature were found to be more frequent and more targeted because cybercriminals made use of sophisticated tactics to permeate weaknesses in security systems and programs.[63]

[61] Ndonga D, 'E-Commerce in Africa, 2012, 256.
[62] Serianu, 2012, 5.
[63] Serianu, 2014, 11.

The year 2016 saw the increase of malware, targeting cell phone and internet banking, which compromised and continues to compromise the safety of users' information on the given. Platforms, where e-commerce is conducted, were attacked with more cybercriminal activity in the form of identity theft and ATM card scamming. Mobile money (MPESA), which is widely used in Kenya, was also targeted by cybercriminals which resulted in major monetary losses as well. During this year it was also discovered that the reason for the overwhelming increase in cybercriminals operating from Kenya is that Kenyan professionals do not have the sufficient tools to explore the ways in which criminals commit these crimes.[64]

Furthermore, a lack of practical regulatory guidance from industry regulators was identified as another contributory factor to the thriving cybercrimes. The issue of enforcement and implementation of regulation surfaced and was attributed to regulation that is not context sensitive but that which is borrowed from other jurisdictions as well as the issue of a lack of education and training among members of law enforcement and the judiciary.[65]

From the reports in 2017, there appeared to be a persistence in the need for better technical training to deal with cybercrime and ultimately achieve a secure cyberspace. This was noted by various industry players namely, Dr Githinji who opines that the lack of specialised academic programmes to meet the cybersecurity needs in the industry. The other issue that was rampant during this reporting period is the malicious spread of 'fake news' which largely affects the vulnerable public who can be manipulated using this information.[66]

Following an eight-year drafting process, legislation known as the *Computer Misuse and Cybercrimes Act* was enacted in 2018. The objective of this Act, as discussed above, is to address is to improve the effectiveness of previous legislation. The *Data Protection Bill* was also promulgated in 2018 with the purpose of ensuring that companies who collect, store and process the data of doing so with permission.[67]

[64] Serianu, 2016, 11.
[65] Serianu, 2016, 12.
[66] Serianu, 2017, 12.
[67] Serianu, 2018, 66.

2.2.2 South Africa

In 2014 it was reported that South Africa was at a loss of an estimated ZAR50 billion resulting from cyber-incidents. In addition to this, that more than one half of a billion records of a personal nature stored online were lost and illegally accessed in the year 2015. These figures were reported by the South African Broadcasting Corporation (SABC) News. In 2011 an approximate ZAR3,7 billion in direct losses and ZAR6,5 billion in indirect losses were recorded. The increase in internet users was estimated to lead to cyber-threats becoming more widespread.[68]

These cyber-threats and malware attacks were, according to the Federal Bureau of Investigations (FBI), by hackers, who targeted financial institutions, private entities including government entities in South Africa, which has been noted as a country among those which have been most vulnerable to cybercriminal activity.[69]

The Department of Telecommunications and Postal Services submitted a report on Cyber-Readiness in which it was provided that organisations should put in place mechanisms to defend against such attacks in their risk management procedures. Hosting training to raise awareness, making changes to policy and technical controls are among the measures that an entity can take. Such initiatives may be a progressive step towards addressing the challenges that have been identified as a lack of skilled individuals and poor awareness among other things.[70] Furthermore, the lack of administrative will, implementation programmes, which are wanting as well as coordination of inter-governmental mandates that are poor, have all contributed to the ineffectiveness of the current laws and policy frameworks developed to address cybercrime issues.[71]

[68] Van Niekerk B, 'An Analysis of Cyber-Incidents in South Africa' 20, *The African Journal of Information and Communication, 2017*, 115.
[69] Schultz CB, 'Cybercrime: An Analysis of Current Legislation in South Africa' published, University of Pretoria, Pretoria, 2016, 12.
[70] *Cybersecurity Readiness Report* 2017, 38.
[71] Gumbi D, 'Understanding the threat of cybercrime: A comparative study of cybercrime and the ICT legislative frameworks of South Africa, Kenya, India, the United States and the United Kingdom' 2018, 11.

2.3 Regulatory Developments in Response to Cybercrime

In 2014 the *Convention on Cybersecurity and Personal Data Protection* was adopted by the African Union. The broad purpose of the convention is to develop a credible cyberspace as well as to respond to the gaps which affect the regulation of the digital environment. The convention also had the objective to establish standards and procedures that seek to respond to the issues arising in cybersecurity in Africa. Such a response includes the harmonisation of legislation. In article 1 of the convention a number of terms are defined one of which being Electronic commerce (e-commerce) which finds relevance to this study. According to the definition in the convention e-commerce constitutes actions that entail offering, buying or the provision of services and goods through the use of computer systems networks for telecommunications such as the internet or other networks which make use of optical, electronic or any other media akin to these for information exchange over a distance. The duty to adopt legislation against cybercrime as well as to facilitate the emergence of national regulatory authorities is provided for in Article 25 of the convention. This Article also provides for the rights of citizens to the extent that the development of frameworks together with the adoption of implementation measures is done in such a way the rights of citizens are not infringed. The protection of critical infrastructure is also provided for in this article which provides that the protection of critical infrastructure involves identifying the sectors in which such infrastructure exists and making provision for the more punitive sanctions for criminal conduct that impacts these infrastructures.[72]

In Article 29 of the convention, the nature of activities which are specific to information communication technologies are provided, and these activities are required to appear as offences in the legislative developments by the member states. These offences include attacks on computer systems which are outlined as gaining access to or attempting to gain access to computer systems when authorised to do so and further to use such access to commit a crime or to facilitate commission of another crime. This article also provides that it is an offence to remain, enter or to make an attempt to remain or enter in a computer system fraudulently. Impacting the functioning of a computer system through hindering or distorting or attempting

[72]Article 1 and 25, *Convention on Cybersecurity and Personal Data Protection*, June 2014.

to engage in such activity as well damaging, altering or deteriorating data in a fraudulent manner are framed as conduct that must constitute offences in the legislation of member states. There is also a requirement to adopt robust regulation for vendors of information communications and technology to ensure that their products have safety guarantee assessments. Computerised data breaches are also contained under this same article and are described as fraudulent interception of data that is computerised from or within a computer system; the use of such data while knowing that it has been obtained through fraudulent means; procuring such data for any person for any benefit should all constitute offences in terms of the convention. Where content-related offences are concerned, this same article provides mainly for child pornography as well as the nature of content that relates to material that is racist, xenophobic or involving the hurling of insults by one group of persons to another. This includes any crimes against humanity such as genocide which are committed through a computer system. The convention then goes further to provide the security measures that ought to be taken for offences that relate to electronic messages and in doing so, states that regulatory mechanisms ought to be developed to ensure that digital evidence is admissible in criminal cases provided that the integrity of such evidence is retained.[73]

Article 30 specifically provides for those ICT-related offences that are applicable to property providing that conduct which entails the violation of property by way of utilising a computer system must constitute an unlawful offence in the legislative frameworks of the member states. Furthermore that the use of ICT in property-related offences shall be considered as an aggravating circumstance for purposes of sentencing after conviction. Under this Article, it is also provided that the regulatory mechanism adopted shall be such that it is not only natural persons that can be held criminally liable but also legal persons. Put differently, these regulatory mechanisms must be framed in such a way that they can be extended to the criminal liability of legal persons.[74]

As a member of the African Union and having ratified this convention, it follows that the legislation developed in Kenya, as well as South Africa, contain similar provisions as those

[73] Article 29, *Convention on Cybersecurity and Personal Data Protection.*
[74] Article 30, *Convention on Cybersecurity and Personal Data Protection.*

that have been required in the convention and that appropriate institutions have been established. The discussion into these two jurisdictions illustrates that the legislative frameworks that have been developed depict what has been provided for in the convention.

2.3.1 Kenya

Preceding the enactment of legislation specially designed to address cybercrime and other cyber matters the *Kenya Information and Communications Act* (*KICA*) was enacted in 1998 and was amended by the *Kenya Communications Amendment Act 2008.* The objective of this Act was the regulation of electronic transactions (e-commerce) and to outline what constitutes offences such as electronic fraud among other offences committed on the internet.[75] Similar to the *Electronic Communications and Transactions Act* (which is discussed in paragraph 2.3.2 below) this Act contains a number of provisions which specifically address issues relating to cybercriminal activity:[76]

- Section 83U provides for unauthorised access to computer data and states that any person who is responsible for causing a computer system to perform a function with the knowledge that he/she is unauthorised to perform such a function, has committed an offence and is, therefore, liable for a fine and/or imprisonment. The section excludes classes of persons including those which are authorised, who act out of a reasonable belief that consent is given and those who rely on statutory provisions in their conduct.
- Section 83V creates an offence out of the access described in section 83U when such access is with the intent of committing a crime in which case it is immaterial whether said person is authorised to access the computer system.
- Section 83W creates offence out of unauthorised access to and an interception to a computer service and outline the liability for such conduct.
- Section 83X provides for unauthorised modification of computer material and states that where any person modifies data with the knowledge that he/she is unauthorised

[75] *Kenya Information and Communications* (Act 2 of 1998).
[76] Section 83U – 84H, Kenya *Information and Communications* (Act 2 of 1998).

to do so, such a person has committted an offence for which he/she is accordingly liable for a fine and/or imprisonment.

- Section 83Y creates an offence out of damaging or denying access to a computer system where the conduct of an unauthorised person accesses a computer system and causes direct or indirect damage to such a system.
- Section 83Z creates an offence out of the unauthorised disclosure of passwords for unlawful purposes.
- Section 84A addresses unlawful possession of devices and data.
- Section 84B creates an offence out of electronic fraud which, according to this section, entails any kind of interference with data with the intention to gain any kind of advantage over another person.
- Section 84C creates an offence out of the tampering of computer codes, computer programmes, computer services and/or computer networks where there is a requirement for such a computer code to be maintained for purposes of the law.
- Section 84D and 84E speak to publishing of obscene information and publishing for fraudulent purposes and creates an offence out of conduct that is of that nature for both of these sections respectively.
- Section 84F deals with unauthorised access into protected systems which provides that it constitutes an offence to secure or attempt to gain secure access to systems that are protected in contravention of the provisions as outlined.
- Section 84H and 84G address offences related to the re-programming of mobile telephones and the possession and supply of anything designed for the purpose of re-programming mobile telephones, respectively. Both sections create an offence out of this defined conduct.

The Act discussed above-containing sections that allude to what is now known as cybercriminal activity is not the only piece of legislation which contains such sections. *The Prevention of Terrorism Act of 2012* also creates an offence out of a terrorist act which entails the use of an electronic system. This is captured in Section 2(a)(vii) which provides that interference with a system that is electronic in nature which causes a disruption in communication supply, transportation, financial or other services which are essential

constitutes a terrorist act. In Section 4, the offence is outlined and the liability for such offence, which in this instance, is a period of imprisonment not exceeding 30 years.[77] One can then imagine how such a provision could act as a safeguard against acts such as cyberterrorism.

This Act was superseded by the *Computer and Cybercrimes Bill* in 2017. This Act was enacted in 2018 as the *Computer Misuse and Cybercrimes Act*. It is similar to the above-mentioned where it defines and creates a criminal offence out of certain conduct; the procedures to enforce its provisions may be found in the *Kenya Criminal Procedure Code*.[78] However, this Act differs from the above-mentioned Act in that it outlines a framework for the prompt detecting, investigating and prosecuting cybercrimes. In addition to this, the Act enhances the penalties for crimes committed using a computer system.[79] For instance hacking; denial-of-service attacks; phishing; infection of IT systems with malware; possession or use of any tools to commit cybercrimes; identity theft or fraud and electronic theft impose penalties ranging from KES200 000 to KES10 000 000. These fines can be imposed with or without imprisonment depending on the circumstances of the case.[80]

The sections in which offences relating to cybercrime are contained in Part III of the Act and are described in brief summations below as follows:[81]

- Section 14 makes provision for unauthorised access and states that a person is guilty of an offence if such person causes a computer system to perform a function whether this is a temporary or permanent state through the infringement of security measures and does so in an attempt to gain access while having the knowledge that such access is unauthorised. According to this section, access is unauthorised if the person accessing the computer system does not have access to the computer system and/or has not obtained the required consent from a person who has the entitlement to gain access into the computer system.

[77] Section 2 and4, *The Prevention of Terrorism* (Act 30 of 2012).
[78] *Kenya Criminal Procedure Code* (Cap 75).
[79] *Computer Misuse and Cybercrimes* (Act 5 of 2018).
[80]Okoth H, Ojango S, 'Kenya: Cybersecurity 2020' *ICLG.com* 2019 https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/kenya on 10 October 2019.
[81] Part III and Part VI, *Computer Misuse and Cybercrimes* (Act 5 of 2018).

- Section 15 addresses access with intent to commit a further offence since it has been established that the conduct in section 14 constitutes an offence, it is then a further offence when a person intends to commit a further offence or to facilitate the commission of a further offence. In this regard, it is not material whether such an offence is committed at the same time or at another time.
- Section 16 deals with unauthorised interference, submitting that it is an offence when a person who has no authorisation intentionally undertakes any act that results in an interference that is unauthorised to a computer system, data or any programme. This particular section also creates an offence out of unlawful unauthorised interference that results in a financial loss that is significant to any person, poses a risk to national security, public health and safety or that which causes the death or physical injury of any person.
- Section 17 speaks to unauthorised interception and provides that when a person without authorisation intentionally undertakes conduct that constitutes a (direct or indirect whether permanent or temporary) interception of the transmission of data over a telecommunication system to or from a computer system, such a person has committed an offence.
- Section 18 pertains to illegal devices and access code and creates an offence out any form of trading (such as procurement, manufacturing, supply) or dealing with devices, data, programmes which are designed for the primary purpose of committing an offence provided for under this Part III is guilty of an offence. This is also applicable to the possession, control or storage of any such devices. This section is qualified by circumstances where there is a valid reason for manufacturing or being in possession of, such as testing a computer system.
- Section 19 provides for unauthorised disclosure of password or access code which creates an offence out of conduct by a person that amounts to the unauthorised disclosure of passwords or access codes to any data that is held on a computer for unlawful gain or purpose or to occasion loss.
- Section 20 makes provision for enhanced penalties for offences involving a protected computer system stating that where Sections 14 to 17 are committed on a protected

computer system which are identified as those that are related to the government there shall be enhanced penalties.

- Section 21 speaks to cyber espionage and it is submitted that a person is guilty of an offence where such a person intentionally and unlawfully performs or authorises or permits another person to commit an offence that entails gaining access as described in section 14 or intercepting data as described in section 17.
- Section 22 relates to false publications and it is provided that when a person intentionally publishes data that is false or misleading or that which misinforms with the intention that the data of this nature will be acted upon as though it were authentic, shall be guilty of an offence.
- Section 23 addresses publication of false information providing that where a person publishes the nature of information described in section 22 above, through forms of media (broadcast, over a computer system) and such a publication has the consequence of chaos, panic or incites citizen violence, is guilty of an offence.
- Section 24 creates an offence out child pornography and states that any person who, through the use of a computer system produces, publishes, possesses, downloads or trades in material that is child pornography has committed an offence.
- Section 25 addresses forgery using computers stating that where a person deletes, alters, inputs or suppresses computer data in a manner that renders such data inauthentic with the intention to have such data acted upon as if it is authentic for legal purposes, that person has committed a punishable offence.
- Section 26 addresses computer fraud stating that where a person unlawfully gains, is responsible for unlawful loss to another person or derives economic benefit for to him/herself or another person through means which entail the use of computer systems (be it impairment, modification, transfer of data or data programmes) such a person is guilty of an offence.
- Section 27 makes provision for cyber harassment and it is submitted that where a person, individually or with a group of other persons, communicates with another person in a manner that affects the person detrimentally, is not decent or is flagrantly offensive in nature, causes the person's apprehension, or causes damage to the person's property, such a person or groups of persons may be held liable.

- Section 28 creates an offence out of cybersquatting, which entails the intentional use of names, business names, trademarks or other word or phrases that are registered, owned or which are utilised by any other person on the internet or existing on another computer network without the necessary authority to do so.
- Section 29 addresses identity theft and impersonation. The section provides that where a person utilises electronic signature, password or any other identifying feature that is unique to any other person commits an offence and may be held criminally liable.
- Section 30 makes provision for phishing, submitting that a person who, for an unlawful purpose or to gain unauthorised access, sends a message through a computer or creates a website through the use of a computer system with the intention of inducing the recipient of the message or the user of the website to disclose personal information, is guilty of an offence and may be held criminally liable.
- Section 31 relates to the interception of electronic messages or money transfers and provides that anyone who undertakes to destroy or abort any electronic mail or any process through which money or information is being conveyed is guilty of an offence.
- Section 32 addresses wilful misdirection of electronic messages when a person undertakes to wilfully misdirect electronic messages engages in unlawful conduct and is, therefore, guilty of an offence.
- Section 33 provides for cyber terrorism stating that where a person accesses a computer system or causes a computer system or network to be accessed with the purpose of carrying out a terrorist act, such a person is guilty of an offence.
- Section 34 addresses inducement to deliver electronic message providing that where a person undertakes to induce a person in charge of an electronic system to deliver any message that is not specifically directed at him/her such a person is guilty of an offence.
- Section 35 makes provision for intentionally withholding a message delivered erroneously and states that where a person detains or hides any electronic mail, message, electronic payment, or debit and credit card, which is found by such a person or erroneously delivered to such a person and ought to be delivered to another person commits an offence.

- Section 36 addresses the unlawful destruction of electronic messages, and it is submitted that any person who undertakes to destroy or abort any electronic mail or process through which money or information is being conveyed, commits an offence.
- Section 37 creates an offence out of the wrongful distribution of obscene or intimate images stating that a person who makes a transfer, endeavours to publish or distribute or download images of another person that are obscene or intimate, through telecommunications networks or any other means that facilitate the transfer of data to a computer system, such a person has committed a punishable offence.
- Section 38 provides for the fraudulent use of electronic data, and it is submitted that a person who does not have authority and knowingly causes another to lose property through the alteration, erasure, suppression or input of data which is stored on a computer, is guilty of an offence. This section provides the same for electronic messages that contain material misrepresentations and the manipulation of computers and electronic device systems with the intention to short-pay or to overpay.
- Section 39 makes provision for the issuance e-instructions which are false stating that where a person issues false electronic instructions while such a person is authorised to make use of computer systems or other electronic devices for financial transactions, such a person is guilty of an offence.
- Section 42 speaks to the aiding or abetting in the commission of an offence and provides that where a person wilfully and knowingly aids or abets the commission of an offence or engages in any preparatory activity in anticipation of or the furtherance of the commission of such an offence, that person is guilty of an offence.

With cybersecurity and cybercriminal activity being multi-jurisdictional concerns, it follows that provision in regulation is made for the trans-border landscape. This Act makes provision for these cross-country offences under the international cooperation framed in Part V. This part broadly provides for mutual legal assistance between the Central Authorities of different States as it relates to undertaking investigations, gathering evidence and expedited preservation of data. Provision is made in Section 61 for mutual assistance regarding accessing stored computer data; trans-border access to stored computer data with consent or

where publicly available in Section 62; mutual assistance in the real-time collection of traffic data in Section 63; mutual assistance regarding the interception of content data Section 64.

The *Data Protection Bill* was passed in 2018 too, and one of the objectives of this bill is to give effect to Article 31 (c) and (d) of the Constitution which speaks to the right to privacy. This bill also seeks to regulate the manner in which personal data is used and to afford protection to data subjects.[82] The year 2019 saw the promulgation of the *Data Protection Act* of Kenya. Section 3 outlines the objects and aims for the provisions as, to regulate how personal data is processed; to ensure that the manner data is processed is consistent with the principles contained in section 25 of the Act; to ensures the protection of individuals privacy; to facilitate the establishment of institutional and legal mechanisms for the protection of personal data; to ensure that data subjects are afforded rights and remedies to protect their data from being processed in a manner that is not consistent with this Act. Where the applicability of the Act is concerned, Section 4 of the Act provides that the Act is applicable to the processing of data subjects located in Kenya.[83]

Despite this progress in the regulatory space, the promulgation of the *Computer Misuse and Cybercrimes Act* has been criticised based on vagueness where definitions of prohibited conduct are concerned, using the prohibition of hate speech as an example of this. Furthermore, there have been questions surrounding what exact powers of surveillance the authorities have and whether these powers could be a violation of privacy which contradicts the *Constitution*.[84]

Shortly after its assent, the Act has also been challenged in a petition by *the Bloggers of Kenya Association (BAKE)* against the *Attorney General and Others*.[85] The BAKE challenged the statute on the basis that it contravenes constitutional provisions namely, freedom of the media; freedom of opinion; freedom and security of the person; freedom of expression; right to

[82] *Data Protection Bill* 2018.
[83] Section 3 and 4, *Data Protection (*Act 24 of 2019).
[84] Muendo M, 'Kenya's new cybercrime laws open the door to privacy violations, censorship' *The Conversation*, 2018 https://theconversation.com/kenyas-new-cybercrime-law-opens-the-door-to-privacy-violations-censorship-97271 on 10 October 2019.
[85] Bloggers Association of Kenya (Bake) v Attorney General & 5 others [2018] eKLR

privacy; right to property and the right to a fair hearing. The high court issued a conservatory order suspending several sections of the Act including:

- Section 5 which speaks to the composition of a committee.
- Section 16 which dealing with unauthorised interference.
- Section 17 dealing with authorised interception.
- Sections 22 and 23 which address false publications and the publication of false information respectively.
- Section 24 which speaks to child pornography.
- Section 27 dealing with cyber harassment.
- Section 28 addressing cybersquatting.
- Section 29 that speaks to identity theft and impersonation.
- Section 31 on the interception of electronic messages or money transfers.
- Section 32 which criminalises wilful misdirection of electronic messages.
- Section 33 dealing with cyber terrorism.
- Section 34 which speaks to inducement to deliver electronic message.
- Section 35 addressing intentionally withholding message delivered erroneously.
- Section 36 creating an offence out of unlawful destruction of electronic messages.
- Section 37 which deals with wrongful distribution of obscene or intimate images.
- Section 38 criminalising fraudulent use of electronic data.
- Section 39 which speaks to issuance of false e-instructions.
- Sections 40 and 41 addressing reporting of cyber threat and employee responsibility to relinquish access codes, respectively.
- Section 42 which outlines aiding or abetting in the commission of an offence.
- Section 48 addressing search and seizure of stored computer data.
- Section 49 outlining record of and access to seized data.
- Section 50 which provides for the production order.
- Section 51 addressing expedited preservation and partial disclosure of traffic data.
- Section 52 dealing with real-time collection of traffic data.
- Section 53 creating an offence out of the interception of content data.

The ruling on this matter is yet to be delivered (January 2020). [86]

The *Law Society of Kenya* (LSK) followed suit in petitioning against the constitutionality of the provisions in the Act with the point of view that the questionable provisions pose a threat to the Bill of Rights where the rights on arrest and prosecution are concerned. One of these rights is the right to freedom of expression in respect of which the LSK highlighted that in a Constitutional democracy, the public has the freedom to state their opinions without those comments or criticisms amounting to hate speech. Furthermore, the LSK contented that the Sections 22 and 23 of Act which address fake news are too broad and vague in the definition of what constitutes falseness. According to the LSK, this has an impact on the right of the public to receive information since the vague definition does not take into consideration that some parts of false information may have value.[87]

Another petitioner, Geoffrey Maina, also challenged the Act following its assent. Mr Maina challenged the Act on similar grounds as the LSK and BAKE, with a focus on the unconstitutionality of the Act being passed without public participation. The petitioner also noted that the sections of the Act that violate the right to privacy could lead to confiscation of property, which constitutes an infringement of the right to have one's property protected. In this petition, the harshness of the penalties was also contented, on the basis that the public may be deterred from making any kind of statement out of fear that a harsh penalty will be imposed.[88]

The overarching idea in the above cases seems to be that the provisions in the Act infringe the rights in the Constitution, which then renders these provisions unenforceable. Whether the court will rule that these sections need revision or not remains uncertain. However, I am

[86] Nanfuka J, 'Sections of Kenya's Computer Misuse and Cybercrimes Act Temporarily Suspended' *CIPESA* 2018 https://cipesa.org/2018/05/sections-of-kenyas-computer-misuse-and-cybercrimes-act-2018-temporarily-suspended/ on 10 October 2019.
[87] Ongeri L, 'LSK challenges the constitutionality of the Computer Misuse and Cybercrimes Act' 2018 https://www.ifree.co.ke/2018/06/lsk-challenges-constitutionality-of-the-computer-misuse-and-cybercrimes-act/ on 10 October 2019.
[88] Wangui V, 'Petitioner challenges the Computer Misuse and Cybercrimes Act' 2018 https://www.ifree.co.ke/2018/06/lsk-challenges-constitutionality-of-the-computer-misuse-and-cybercrimes-act/ on 10 October 2019.

inclined to agree that these are valid concerns because difficulties to enforcement, as discussed, are likely to arise where there are contradictions in legislation as well as vagueness the meaning of provisions in the law to be enforced.

2.3.2 South Africa

The South African common law (Roman-Dutch Law to be specific) outlines theft, housebreaking and malicious injury as crimes. However, their definitions have proved to be unsuitable and narrow to apply in the context of cybercrime, which typically involving tangibles, while the crimes in terms of the common law point to intangibles. Before the promulgation of any legislation that specifically addresses cyber matters, the common law and existing statutory laws were applied.[89]

In the case of *S v Howard*, this is illustrated where the court undoubtedly reached the decision that causing the breakdown of an entire information system constituted malicious injury to property. Furthermore, the element of physical property did not have to be present in order for the definition of a crime to apply to criminal activity where all other components are present.[90] While the courts extended the scope of the common law to find application to cybercriminal matters, the regime was found wanting, as it has inherent limitations. To respond to this lack the South African Law Commission (SALC) undertook an investigation in which it sought to establish whether the common law and other statutory provisions were suitable and if not whether there was a need to develop a regulatory framework that speaks directly to cybercriminal activity. Following its investigative efforts, the SALC reached and submitted the conclusion that a regulatory framework was required to address cyber issues more directly as opposed to a system where the scope of common law is extended to apply to

[89] Cassim F, 'Addressing the Challenges posed by Cybercrime: a South African Perspective' 5(3) *Journal of commercial Law and Technology*, 2010, 118.
[90] *S v Howard* (Case no. 41/ 258 / 02) Johannesburg Regional Magistrates Court, Unreported.

cybercrime.[91] These limitations identified in the common law in relation to addressing the internet crimes then prompted the promulgation of the *ECTA* as well as the *RICA*.[92]

The *RICA* was enacted with the view of mainly protecting those who have had their communications unlawfully intercepted as well as ensuring that SIM cards for cell phones and these cell phones are possessed lawfully. Thus, anyone who does not have authorised possession thereof can be held liable under this piece of legislation. The protective element of the Act is evident from the clear-cut definitions of direct and indirect communications as well as those that cannot be intercepted. It would follow that a party who intercepts those communications which cannot be intercepted is then in violation of the provisions of this Act.[93]

Despite developments brought about by this Act, a number of gaps were identified, one of these being that its application was restricted to the borders of South Africa, which is unsuitable for crimes committed on the internet, seeing that they tend to be of a multi-jurisdictional nature. The other limitation identified was that the Act would rapidly become obsolete because of cybercriminals developing innovative ways to engage in illicit activity.[94]

As the name suggests the *ECTA* was promulgated to regulate electronic communications, including transactions to ensure that these are facilitated in a manner that upholds interest of the public. Cybercrime is outlined in chapter 13 of the Act and a focus is placed on accessing, intercepting, extorting, forging and fraudulent conduct through the use of an electronic platform. This chapter contains Sections 85 to 89, and each section addresses a different aspect that alludes to cybercrime:[95]

---

[91] Van der Merwe D, 'A Comparative Overview Of The (Sometimes Uneasy) Relationship Between Digital Information And Certain Legal Fields In South Africa And Uganda' 17(01) *Potchefstroom Electronic Law Journal,* 2014, 310.
[92] Schultz CB, 'Cybercrime: An Analysis of Current Legislation in South Africa' published, University of Pretoria, Pretoria, 2016, 16.
[93] Chapter 9, *Regulation of Interception of Communications and Provision of Communication-Related Information* (Act 70 of 2002).
[94] Watney M, 'The Evolution of Internet Legal Regulation in Addressing Crime and Terrorism' 2(2) *Journal of Digital Forensics, Security and Law* 2007, 52.
[95] Chapter 13, *Electronic Communications and Transactions* (Act 25 of 2002).

- Section 85 defines access to include conduct by a person who takes note of data and continues to access such data in spite of becoming aware that he/she is unauthorised to access such data.
- Section 86 addresses unauthorised access to, interception of or interference with data. Subsection (1) creates an offence out of intentionally accessing or intercepting any data without permission or authorisation to do so. Subsection (2) creates an offence out of the conduct as described in subsection (1) in a manner that causes such data to be modified, destroyed or rendered ineffective in some way. Subsection (3) creates an offence out of conduct which seeks to defeat the security measures of a system or to otherwise disregard passwords in order to gain entry into a system. Subsection (4) creates an offence out of the conduct, outlined in subsection (3) as a means to unlawfully defeat security measures, which are specifically designed to protect data. Subsection (5) creates an offence out of conduct with the intent to deny service to legitimate users.
- Section 87 addresses fraud, extortion and forgery which are computer-related. Subsections (1) and (2) of this section create an offence out of performing or attempting to perform any of the aforementioned actions seeking to obtain an unlawful advantage with the intention of presenting any data or information in a fraudulent manner.
- Section 88 provides that any person who attempts to or aids and abets any other person attempting to commit any of the afore-mentioned offences is guilty of an offence.
- Section 89 of this Act then provides the penalties for the conduct provided for above. These penalties range from periods not exceeding 12 months, periods not exceeding five-year imprisonment as well as the imposition of fines.

One can see from the cybercrimes covered under this Act that there was no adequate coverage of the broad range of cybercrimes that can be committed on the internet. This inadequate cover also reveals the gap akin to the *RICA* concerning cybercriminals engaging in illicit activity at rapid rates thus causing the legal regulatory frameworks to lag behind the cybercriminal activity. This gap then renders regulation insufficient.

The *Protection of Personal Information Act* that was promulgated in South Africa in 2013 seeks to address matters that relate to data protection, such as breaches of security, discrimination, and theft. Section 2 of the Act provides the purposes of the Act which may be briefly outlined as follows: to protect the right to privacy which is a Constitutional right through safeguarding information when a responsible party processes it within the ambit of limitations which is justifiable, such as the free flow of information; regulating the manners in which information of a personal nature is processed ensuring that there are requirements for information to be processed lawfully; provision of rights and remedial measures for persons to protect their personal information from processing that is in contravention with the Act; the establishment of measures to ensure that the rights provided for in the Act are well observed.[96]

A comparison has been drawn between this piece of legislation and the *General Data Protection Regulation*, which was put forward by the European Union.[97] When analysing these provisions, one can note the similarity found in the regulations which are in the provisions appearing in both of the frameworks, specifically those addressing the rights of data subjects, lawful processing of information procedures as well as the recognition of information flows which are of trans-border nature.

The year 2015 saw the publication of the National Cybersecurity Policy Framework (NCFP) by the Minister of Security. The overarching purpose of the framework is to create a cyber environment or space that is secure and reliable as well as to facilitate and protect this environment to the extent that national security imperatives and the economy are supported. The South African Government outlines the following specific aims and objectives for this framework: to achieve centralised coordination of activities relating to cybersecurity through the facilitation and establishment of policy frameworks, structures as well as strategies to support cybersecurity. The Government also seeks to foster coordination and cooperation between itself, civil citizens and the private sector so that there is a robust interplay between policy, legislation, technology and societal acceptance. Promotion of international

[96] Section 2, *Protection of Personal Information* (Act 4 of 2013).
[97] *Protection of Personal Information* (Act 4 of 2013)

cooperation and a culture of cybersecurity; development of skills and research capacity, also, to promote compliance and adherence to the appropriate technical cybersecurity standards.[98]

The *Cybercrimes and Cybersecurity Bill* creates an offence out of a wider scope of criminal offences than those which were discussed above under the *ECTA.* These offences are contained in the second and third chapters of this Bill. These sections may be summarised as follows: [99]

- Section 2 makes provision for unlawfully securing access and states that any person who gains unlawful and intentional access to a computer program, computer system or computer data has committed a punishable offence. It is further provided under this section that access, which is secured by a person, who affects the computer data, program or system, while the access secured is unauthorised, is guilty of an offence. Access is unauthorised where it is not lawfully secured, where there is no lawful consent obtained and where the limits of the consent or entitlement given, are exceeded.
- Section 3 addresses unlawful acquired data and provides that where a person unlawfully overcomes a protection measure on a computer system and, as a result, is able to acquire data from or within or to a computer system, such a person is guilty of an offence. This measure is also applicable to data that are possessed under these same circumstances. Furthermore, if it is reasonably suspected that the data possessed have been acquired through unlawful means and the person in possession fails to account for such data, such a person may be guilty of an offence.
- Section 4 deals with unlawful acts in respect of software or hardware tools and provides that any person, who unlawfully possesses or deals (manufacturing, supply) of software or hardware tools, and makes use of these tools to commit any of the offences in Section 2 above, is guilty of an offence. Software and hardware tools are understood to mean electronic and mechanical instruments or devices.
- Section 5 describes unlawful interference with data or a computer program and states that a person is guilty of an offence if such person unlawfully interferes with data or a

[98] Government Gazette 609, 2015, 12
[99] Chapter 2 and 3, *Cybercrimes and Cybersecurity Bill (*2017).

computer program. The section then goes further to describe this interference to constitute that which permanently or temporarily affects (deleting, damaging, altering, obstructing) the computer program or data.

- Section 6 addresses unlawful interference with a computer data storage medium or computer system, and under the section, it is submitted that any person who engages in such conduct is guilty of an offence. Such an interference is understood as that which causes an interruption or impairment to the computer data storage medium or computer system.
- Section 7 addresses unlawful acquisition, possession, provision, receipt or use of password, access codes or similar data or devices and create an offence out of illicitly engaging in any of the conduct as described in Sections 2, 3, 5, 6, 8, 9 with the passwords, access codes or similar data or devices that have been unlawfully acquired, possessed, provided or received.
- Section 8 makes provision for cyber fraud, and it is stated that where a person intentionally and unlawfully makes a misrepresentation using data and a computer program or by way of interfering with data or a computer program, such a person is guilty of an offence. Such a misrepresentation must have caused or potentially caused prejudice.
- Section 9 addresses cyber forgery and uttering and provides that a person who makes false data or a false computer program causing prejudice or potential prejudice to another person intentionally, unlawfully, and with the intention to defraud, is guilty of an offence. This is also applicable where a person who passes on false data or a false computer program with the intention to defraud, this is also applicable.
- Section 10 addresses cyber extortion, and it is submitted under the section that where a person intentionally and unlawfully commits or threatens to commit specific offences contained in this chapter (Sections 3, 5, 6, 7) with the aim to obtain any advantage over another person or in an attempt to compel another person to perform or abstain from performing any act, such a person is guilty of an offence.
- Section 11 outlines aggravated offence, stating that offences committed through the use of a restricted computer, the person committing the offence is guilty of an aggravated offence. Restricted computers are described as those which are under the

exclusive control of financial institutions, critical infrastructures and organs of state. Unlawful conduct that grossly impacts the citizens of the Republic is also considered to constitute aggravated offences.

- Section 12 speaks to attempting, conspiring, aiding, abetting, inducing, inciting, instigating, instructing, commanding or procuring to commit an offence, and provides that a person is guilty of an offence where such person attempts, conspires with another person, incites, instigates, instructs, commands or procures another person to commit any offence outlined under this chapter.
- Section 13 speaks to the theft of incorporeal, and it is provided that the common law of theft must be understood to be inclusive of conduct that entails the theft of incorporeal.
- Sections 14 and 15 provide a comprehensive outline of the penalties and the competent verdicts that are applicable to the different offences, respectively.
- Section 16 makes provision for data messages which cause damage to property or violence and states that a person is guilty of an offence where such a person makes use of a computer to make available, broadcast or distribute a data message to a specific person or group of persons or the general public and this is done with the intention of damaging property or inciting violence against person.
- Section 17 addresses data messages which are harmful, and submits that a person who unlawfully and intentionally makes use of a computer to make available, broadcasts or distribute data messages of a harmful nature is guilty of an offence.
- Section 18 makes provision for conduct involving distributing data messages of intimate images without the required consent, and it is stated that a person is guilty of an offence where such person who makes use of a computer system to unlawfully and intentionally make available, broadcast or distribute data messages which contain intimate messages of an identifiable person who has not given consent to such broadcast or distribution. In terms of this section, intimate messages are those in which the person depicted, is nude, with genital, anal organs and breasts are exposed.

As it has been alluded to in preceding paragraphs, jurisdiction is of particular importance where the cyberspace and cyber matters are concerned. The Bill mentioned above addresses

jurisdiction in Chapter 4, Sections 23 which provides that (Section 23(2)) the courts in the Republic of South Africa have jurisdiction over cybercriminal matters concerning citizens and ordinary residents who are outside of the Republic at the time which such offences are committed even in instances where such conduct does not constitute an offence where it is committed. Furthermore, in Section 46, provision is made for the circumstances under which foreign requests for assistance and cooperation may be made.[100]

It appears that this Bill acts as an extension of the *ECTA*, in that most of its provisions are similar to those contained in the *ECTA*, with more areas covered than in the *ECTA*. This extension can be seen in the provision which relates to jurisdiction in Section 23, which indicates that South African courts will have extra-terrestrial jurisdiction in certain circumstances.[101] This progressive step attempts to address the jurisdictional issues that often arise with cybercrime, as I have alluded to in the preceding chapter (1.5).

The regulatory mechanisms discussed above have not been without contestation, which can be seen in the case law relating to these statutes. The Amabhungane Centre for Investigative Journalism presented a case before the court upon the discovery that one of their journalists had been surveilled on an unauthorised basis. The organisation claimed that the sections in the *RICA* which allow for such surveillance, essentially spying, are unconstitutional. The judge presiding over this case ruled in favour of this organisation and ordered that such surveillance be put to a stop; that new wording be inserted into the Act such that only surveillance is authorised where the person is informed after a defined period of time; and that these various changes are to be in effect up until such time when Parliament passes an amended Act or a new piece of legislation completely.[102] From this decision the significance of role of the judiciary can be seen where developing regulatory frameworks is concerned.

[100] Chapter 4 and 6, *Cybercrimes and Cybersecurity Bill (*2017).
[101] Section 23, *Cybercrimes and Cybersecurity Bill (*2017).
[102] < https://businesstech.co.za/news/technology/341219/high-court-finds-that-south-africas-surveillance-act-rica-is-inconsistent-with-the-constitution/ > on 16 December 2019.

2.4 Structural Developments to Address Cybercrime

2.4.1 Kenya

Several institutions which can influence the policy-making have emerged with the rapid development in the information and communications and technology space in Kenya, a few of these are worth mentioning in this study.

In 2007, the Kenya ICT Board was established following a Presidential Order. The purpose of the board is to develop ICT in Kenya, particularly in the business process outsourcing (BPO) and the services which are enabled by IT.[103]

The ICT Authority was established in 2013 to, mainly, enhance the manner in which the government supervises electronic communication as well as to enforce ICT standards as set by the authority.[104]

In 1999 the Communications Authority of Kenya was established in terms of the *KICA* with the purpose of making possible the development of the sector which relates to communications in Kenya. This communication includes several areas with cybersecurity and electronic commerce[105] being those which are relevant to the study.

Article 240 of the *Constitution* establishes a National Security Council which is mandated with supervisory control over organs for national security in the Republic of Kenya.[106]

The Kenya Computer Security Incident Response Team (CSIRT-Kenya), also established in terms of the *KICA* and forms part of the framework for national cybersecurity management. It is comprised of law enforcement agencies working together with the Communications

[103] Waema TM, 'Ndung'u MN Understanding What is Happening in ICT in Kenya' Research ICT Africa, Policy Paper, 15, 2012, https://researchictafrica.net/publications/Evidence_for_ICT_Policy_Action/Policy_Paper_9_-_Understanding_what_is_happening_in_ICT_in_Kenya.pdf on 10 October 2019.
[104] < http://icta.go.ke/ > on 17 December 2019.
[105] < https://ca.go.ke/about-us/who-we-are/what-we-do/ > on 17 December 2019.
[106] Article 240, *Constitution of Kenya* (2010).

Authority to address matters of cybersecurity both on a local level and an international level.[107]

2.4.2 South Africa

Similar to the Kenyan landscape, various institutions have emerged to promote cybersecurity in South Africa. These institutions are outlined below.

The establishment of the Critical Infrastructure Council is proposed in Section 4 of the *Critical Infrastructure Protection Bill*, and it is in Section 7 of this Bill that the function of such a council is provided. These functions are broadly of an advisory nature on matters that relate to identifying, assessing and managing critical infrastructure among other important functions. The section states that the council is to advise the Minister on guidelines as they relate to the identification, assessment, management of risks associated with critical infrastructure; the development of transparent processes and the development of policies to declare and protect critical infrastructure, while bearing in mind the budgetary implications; receive and consider applications for declarations of critical infrastructure; submit recommendations to the Minister on matters regarding critical infrastructure; review risk assessments and compile reports to the Minister as well coordinate Government departments and the private sector, among other functions.[108]

There is also the Cybersecurity Response Committee, which is led by the Director-General of the State who is assisted by those heading relevant agencies and departments, was mandated with strategising and making decisions as well as prioritising areas that require intervention based upon assessments conducted to identify threats.[109]

The Centre for Cyber Security was established by the University of Johannesburg together with the Academy of Computer Science and Software Engineering as an initiative to respond to cybercrime in Africa. This centre seeks to deliver services in the Cyber Security space as

[107] < https://www.ke-cirt.go.ke/index.php/services/national-cirt-services/ > on 17 December 2019.
[108] Section 7, *Critical Infrastructure Bill* (2017).
[109] Van Niekerk B, 'An Analysis of Cyber-Incidents in South Africa' 87.

well as in Critical Information Infrastructure Protection to interested actors in Southern Africa.[110]

The South African National CSIRT is the Cyber Security Hub which aims to create an environment that is safe for all residents to communicate, to socialize and to transact. One of the ways which it does this is through providing information to raise awareness to all residents.[111]

2.5 Conclusion

The discussion in this chapter provides an outline into the efforts that have been made on a regulatory level as well as the institutional frameworks that have mushroomed as a means to address the issue of cybercrime to create a safe cyber environment. This is done by viewing the legislative frameworks that have developed in recent years in both jurisdictions and also through viewing the institutions that have emerged with respect to cyber matters. The purpose behind discussing the two jurisdictions in the same chapter is primarily that both form part of the African dispensation and can, therefore, present a perspective on the African landscape and also that the similarity seen in the developments made in each jurisdiction over the recent years.

From the discussion, it appears that various efforts have been made where developing legislative frameworks is concerned. However, the literature suggests that there are fewer institutions to address the cybercrime issue. This predicament may be attributed to several issues that the African continent is faced with. Such issues tend to be the central focus, which then creates an environment where efforts towards the resolution of other issues that are viewed as secondary ones, such as cybercrime, are not as rigorous as those efforts seen towards the primary issues. This position is unfortunate because the recent reports (as outlined in the discussion) show that the issue of cybercrime persists and is still pervasive in Kenya as well as well as in South Africa. The persistence of cybercrime impacts the potential contribution that can be made by e-commerce to African economies.

[110] <https://adam.uj.ac.za/csi/About.html > on 17 December 2019.
[111] <https://www.cybersecurityhub.gov.za/ > on 17 December 2019.

Chapter Three: Regulatory and Institutional Developments in the United Kingdom (International Perspective)

3.1 Introduction

The preceding chapter provides insight into the current regulatory landscape in Kenya and South Africa, which have been identified as African states with developing economies. When viewing the landscape of these states respectively, one can note that the development in the regulatory space is moving at relatively similar paces, therefore, impacting the use of e-commerce in similar ways. It is for this reason that it becomes important to provide insight into a regulatory framework in a developed nation where one can see the benefits of regulation and institutions to e-commerce activity.

In this chapter, I have provided an extensive discussion of the regulatory frameworks and institutional developments in the UK that are relevant to cyber matters.

I have then proceeded to analyse the criticisms made against these developments and provide the shortcomings of these developments in achieving the objective of cultivating a secure cybersecurity space. This is done through a comparative analysis of each jurisdiction that has been discussed in preceding chapters, with Kenya and South Africa viewed as providing an African perspective, and the UK providing an international perspective.

3.2 Contextual Issues Relating to the United Kingdom

In 2017, the British government valued e-commerce sales in the UK at 586 million British Pounds.[112]The e-commerce industry continues to boom in the UK, at a much faster pace than in developed countries, as one would imagine. It is largely dominated by American companies, but even so, local companies have penetrated the e-commerce space, which is considered to be a sophisticated market. The market comprises traditional retailers as well as those that operate purely on the internet: Debenhams is among these as are Currys PC World;

[112] < https://www.statista.com/topics/2333/e-commerce-in-the-united-kingdom/> 03 February 2018.

John Lewis and Partners; Marks & Spencer; Tesco; Asda; Argos; Asos; eBay UK; Amazon UK, all cited as the leading stores in the e-commerce industry.[113]

The traditional brick-and-mortar model for retail was somewhat threatened by the consequences of Brexit and its implications for the stores in Europe. The uncertainty surrounding this issue brought more activity to the e-commerce market, as predictions indicated that consumers are likely to spend more online. This activity puts both traditional and e-commerce retailers in a favourable position, and also highlights the benefit of e-commerce platforms acting as alternatives to traditional ways of shopping.[114]

While the use of e-commerce promises economic growth, various factors may inhibit this potential growth. These factors have been alluded to above in the context of developing countries and can also be seen in more developed contexts. Trust is one of these factors, and it is vital to business-to-consumer e-commerce because consumers enter into transactions for goods or services with internet traders based on trust that there will be delivery. Once trust is established consumers may be encouraged to form long-lasting relationships with retailers which is beneficial to the e-commerce market. Awareness, perceived utility and accessibility are also a relevant factor in that when consumers have knowledge about e-commerce options and view these as useful and accessible facilities, they are more likely to engage. Governments have an important role to play in this industry as they are responsible for institutions and ICT infrastructure to support the growth of e-commerce for the benefit of a given economy by safeguarding the security of consumers because cybercrimes, such as fraud and hacking, are a significant impediment to the development of e-commerce across the board.[115]

The UK fell victim to what was categorised as one of the world's worst cybercrime incidents in 2017, when it was hit by the WannaCry ransomware virus, known as the most widespread attack orchestrated by hackers who navigated their way into the National Health Service computer system resulting in hospitals and medical staff having to operate their day-to-day

[113] < https://disfold.com/top-e-commerce-sites-uk/> on 03 February 2020.
[114] < https://www.e-xanthos.co.uk/blog/ecommerce-uk-online-retail-trends> on 04 February 2020.
[115] Kabango CM, Asa R, 'Factors influencing e-commerce development: Implications for the developing countries' 1(1) *International Journal of Innovation and Economic Development*, 2015, 65 -66.

functions completely offline, essentially caused a shutdown. This National Health Service computer system was down for several days until the kill switch was located by a security researcher.[116]

The UK Office for National Statistics issues a Crime Survey on an annual basis. In the latest survey released for the year ending in March of 2018 following the case, it was submitted that an approximate 4 million cybercrimes were committed in England and Wales combined, over a period of 12 months. Within this approximation, an estimate of 3 million of the crimes were offences related to fraud and the remaining approximation of 1 million relating to computer misuse, which specifically comprised child pornography and hacking. There is also evidence that different categories of cybercrimes are more common than others with each year. Not all this is bad news, however, because the report also provided that these statistics indicate a 31% reduction in cybercrime which can be attributed to more advanced antivirus technology. Despite this progress, the UK is warned against complacency because cybercriminals develop more sophisticated means to achieve their illicit ends, thus putting users in a constant state of vulnerability.[117]

3.3 Regulatory Mechanisms in Response to Cybercrime

The Council of European Union (EU) Convention on Cybercrime was adopted in 2001 which in section 1, Chapter II contains the offences which are considered to be against the confidentiality, integrity and availability of computer and data systems as follows:[118]

- Article 2 addresses illegal access and provides that the parties shall adopt measures under their domestic law, such as criminal liability, for the intentional access to a computer system with the right to access such a computer system. Such an offence may be committed through the breach of a security system or other unscrupulous intent, which involves the use of a computer system.

[116] < https://www.thesun.co.uk/tech/4120942/five-of-the-worst-cases-of-cyber-crime-the-world-has-ever-seen-from-data-theft-of-one-billion-yahoo-users-to-crippling-the-nhs/> on 03 February 2020.
[117] < https://www.tigermobiles.com/blog/cybercrime-statistics/> 04 February 2020.
[118] Article 2 to 11, *Council of Europe Convention on Cybercrime*, November 2001.

- Article 3 makes provision for illegal interception and provides that each party shall adopt measures under their domestic law that are necessary to establish criminal offences for conduct that involves the unlawful interception of computer data made by technical means, which include electromagnetic emissions from a computer system carrying such data.
- Article 4 provides for data interference and states that each party shall adopt measures under their domestic law that are necessary to establish criminal liability for interfering with intentionally and without right with data in a manner that causes such data to be damaged, deleted, deteriorated, altered or suppressed.
- Article 5 addresses system interference and provides that each party shall adopt measures under their domestic law that are necessary to create criminal offences relating to, intentional conduct that results in the serious hindering of the functioning capacity of a computer system through the input, transmission, damage, deletion, deterioration, alteration or suppression of computer data.
- Article 6 makes provision for the misuse of devices and provides that each party shall adopt measures necessary to establish criminal offences under their domestic law for conduct that relates to producing, procuring for use, selling, importing, distributing or otherwise making available devices, computer programmes, access codes, computer password with the intention to commit offences and without right to do so.
- Article 7 addresses computer-related forgery. It provides that each party shall adopt measures, under their domestic law, to establish criminal liability for the intentional conduct of inputting, altering or deleting computer data which results in inauthentic data that with the intention that such data be acted upon for legal purposes as if it were authentic.
- Article 8 provides for computer-related fraud and provides that each party shall adopt measures under their domestic law to establish criminal liability for conduct that is undertaken with the intention and causes the loss of property to another through inputting, altering, deleting, suppressing or any interference with computer data with the intention to fraudulently obtain economic benefit for oneself or another person.
- Article 9 addresses offences related to child pornography and states that each shall adopt measures under their domestic law to establish criminal offences for conduct

that entails producing, making available, transmitting, procuring and possessing material that depicts minors and persons appearing to be minors engaged in conduct that is sexually explicit.

- Article 10 provides for offences related to infringements of copyright and related rights stating that each party shall adopt measures under their domestic law that creates a criminal offence out of the infringement of copyright and such related rights.
- Article 11 makes provision for attempt and aiding or abetting and states that each party shall adopt measures under their domestic law to create criminal offences out of the intention attempting and aiding or abetting of any the offences that have been outlined from Articles 2 to 10 above.

In 1995 the European Parliament and of the Council of the European Union adopted the directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data which is no longer in force, with its validity ending in 2018. It was replaced by the Regulation of the European Parliament and of the Council of the European Union on the protection of natural persons with regard to the processing of personal data and on the free movement of such data in 2016 otherwise known as the General Data Protection Regulation (GDPR).[119] Where data protection is concerned, the *Data Protection Act* was also enacted in the UK in 2018.[120]

Article 1 of the regulation provides that it is a fundamental right of natural persons to be protected with respect to the processing of data that is relevant to such persons. The right to be extended this type of protection is contained in the Charter of Fundamental rights of the European Union. Article 2 provides that where the principles of data protection are concerned and the protection of data subjects should not be contingent on the nationality or residence of data subjects and should rather be focused on respecting the rights and fundamental freedoms of data subjects. Article 3 of the GDPR addresses the territorial scope of the regulation.[121] Despite the consequence of Brexit being that the UK no longer forms part of the EU, the

[119] <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32016R0679> on 03 February 2020.
[120] *Data Protection* (Act of 2018).
[121] Article 3, *General Data Protection Regulation*, April 2016.

GDPR, as well as other EU regulations, find application to the UK as it will be deemed as part of the EU until December 2020 where this period may or may not be extended.[122]

Richard Lloyd brought a class action on behalf of over 4 million Apple iPhone users, against Google LLC before the Court of Appeal. The background to this case is briefly that, from 9 April 2011 to February 2012 Apple iPhone users were impacted by the Safari Workaround. The Safari Workaround enabled Google to set a DoubleClick Ad cookie on devices without device users consent or knowledge resulting in Google having access to information concerning users' internet activity, including information on the approximate geographical location of users. Prior to proceeding with the claim Lloyd sought permission from the High Court to institute the claim for damages outside of the jurisdiction however this was refused by the court. Lloyd appealed this decision and was duly granted this permission by the court of appeal making reference to both the GDPR and Data protection Act of 2018.[123] This judgement is particularly significant as it sets a precedent for claims to be instituted outside of a jurisdiction when the circumstances allow it.

In addition to the GDPR and the Convention referred to above, as a regulatory mechanism applicable to the UK, laws related to cybercrime also exist within the UK. These laws have been promulgated over the years. In 1990, the *Computer Misuse Act* was promulgated, with the view of mainly providing for ensuring that computer material is secured against modification and access thereto which is unauthorised.

The first section of the Act deals with access to computer material that not authorised and provides that a person has committed an offence where he/she prompts a computer to perform any function that causes him/her to secure access to computer data or program. The section goes further to provide that at the time that such access is secured the person is unauthorised to secure the access and has the knowledge that he/she is not authorised. Penalties relating to this described conduct also appear under this section. The second section

[122] <https://www.itgovernance.co.uk/eu-gdpr-uk-dpa-2018-uk-gdpr> on 03 February 2020.
[123] *Lloyd v Google LLC* (2019), The Court of Appeal of the United Kingdom.

of the Act deals with the unauthorised access into a computer system with the intention to commit or facilitate the commission of a further offence. It follows that this is considered a 'further offence' because it has been established the section one constitutes an offence. Furthermore, this section provides that this conduct need not be committed at the same time or on the same occasion as the conduct outlined in section one. Additionally, that the commission need not be possible for a person to have met the requirement to be guilty of an offence. In other words, that the intention to engage in illicit conduct is enough to establish that an offence has been committed. Section three of the Act creates an offence out of the unauthorised modification of computer material. At the time that the offence is committed the person must have the requisite knowledge and the requisite intent which, according to the section, constitutes an intent to modify data in a manner that impairs the computer or computer program. This is also applicable to an intent to prevent or hinder access to data or program held on the computer.[124]

In the fourth section of the mentioned Act, jurisdiction is described, and the territorial scope of the Act is outlined. According to this section, this Act applies to the home country of the UK being Scotland, England, Northern Ireland and Wales. It then goes further to state that for conduct to be considered an offence in the UK, there must be a link with the domestic jurisdiction. This link can either be the accused being in the home country at the time the offence is committed or the computer that the accused sought to secure unauthorised access to being in the home country at the time the offence was committed.[125]

Electronic communications are dealt with under Electronic Communications Networks and Services which appear under Chapter one of the *Communications Act* of 2003. Section 125 of this Act states that a person is guilty of an offence if he/she obtains electronic communications services and does so with the intent to avoid payment of a charge related to the use of that service. Further that it is an offence where a person possesses or supplies apparatus with the intention to aid the contravention of Section 125. In Section 127, an offence is created out of

[124] Section 1 to 3, *Computer Misuse* (Act 1990).
[125] Section 4 and 5 (Act 1990).

the improper use of a communications network such as sending messages that are of a gross or obscene nature.[126]

The *Civil Contingencies Act* of 2004 is concerned with making provision for civil contingencies. Cybercrime protection and the achievement of cybersecurity is relevant to Section 19 of this Act, which outlines what constitute emergencies and, therefore, requires arrangements for contingency. An event which threatens serious damage to the security of the UK, such as a disruption to a system for communications, is captured under this section.[127]

One can see that these pieces of legislation, having been promulgated over a decade ago and some more than that, may need to be revised to be adequately applied to the current dispensation. The Criminal Law Reform Now Network (CLRNN) submitted a lengthy report calling for the revision of the *Computer Misuse Act* discussed above. The CLRNN cited the following reasons for the recommendation that an updated version of the legislation is needed: issues with enforcement of the provisions contained in the Act as well legal obstructions that could place critical infrastructure in the UK in a vulnerable position; further, the provisions of the Act are framed in a manner that exposes cybersecurity professionals to criminal prosecution for doing their required work. The CLRNN thus recommends that defences for such professionals as well as those for professionals conducting research around cybercrime and cybersecurity be built into the updated Act such that there is no exposure to criminal prosecution for professionals undertaking this type of work.[128]

During 2018, it was announced that plans were underway for the building of specialised courts for cyber matters, fraud and economic crimes. This step was viewed as promising towards the fight against cybercrime, as matters will be brought before presiding officers who

[126] Section 125 to 127, *Communications* (Act of 2003)
[127] Section 19, *Civil Contingencies* (Act of 2004).
[128] Bowcott O, 'Cybercrime laws need urgent reform to protect UK, says report' 22 January 2020 <https://www.theguardian.com/technology/2020/jan/22/cybercrime-laws-need-urgent-reform-to-protect-uk-says-report> on 04 February 2020.

are well-informed about cyber matters and a specialised court will allow for the tracking of case law to be done with less complexity.[129]

One of the most significant cybercrime prosecutions was seen by the UK in 2018 when 21-year-old hacker, Alex Bessell was incarcerated for the commission of over two thousand offences. The offence was prosecuted in terms of the *Computer Misuse Act*. Bessell generated copious amounts of money from trading his as well as others' malware products which enabled the creation of viruses, launching of cyber-attacks and theft of data by users. In addition to this, Bessell created a shop for online hackers on the dark web.[130]

3.4 Structural Developments to Address Cybercrime

With the rise in computer use and the development of cybersecurity measures against cybercriminal activity various institutions, strategies and directives emerged in the UK to work hand-in-hand with, and to give effect to the legislative frameworks developed. Where strategies are concerned a National Security Capability Review was commissioned in support of a National Security Strategic Defence and Security Review was implemented in 2015 with a national security defence doctrine intended to report on security issues that will demand the government's attention over a decade. Cybersecurity issues will form part of these priority issues and are captured as such in the review.[131]

In 2016, a National Cybersecurity Strategy 2016 - 2021 was implemented in the UK. The strategy outlines the UK government's plan to create secure and resilient cyberspace within the UK. Two years following its implementation, a report was issued on its progress which contains the strategic outcomes of the strategy itself. These outcomes include: understanding the threat; tackling cybercrime through responding and deterring cybercriminals; ensuring that the UK has the capacity to respond to and manage cybercrime incidents; to establish an active cyber defence to render categories of cybercrimes ineffective; ensuring that technology is secure by designing cybersecurity features into products and services; improving the

[129] < https://www.pinsentmasons.com/out-law/news/cyber-crime-london-cyber-court-plans> on 03 February 2020.
[130] < https://www.bbc.com/news/uk-england-42733638>on 03 February 2020.
[131] *National Security Capability Review*, 2015, 10.

cybersecurity of government to ensure that networks are secure; management of the cyber risk in the economy and society; develop the cybersecurity such that cybersecurity can be sustained as well as developing the skills pipeline in the sector; research and planning towards ensuring the achievement of these objectives.[132]

The National Risk Register has the purpose of assessing significant emergencies that pose a threat or have an impact on all or major parts of the UK and its citizens. These risks are placed into different categories, one of which being 'malicious attacks.' Malicious attacks in this context are understood to include those which are launched using technological means[133] thus amounting to cybercriminal activity.

In order to remain resilient to cyberattacks and sustain cybersecurity for the financial services sector in the UK, the Bank of England Sector Cyber Team in collaboration with the Council for Registered Ethical Security Testers (CREST) established the CBEST Vulnerability Testing Framework, which is a sophisticated security testing system. This initiative is the first of this nature to be spearheaded by any central bank in the world, thus placing the UK in the position of a trailblazer in this regard. This system promises to bring benefits to the financial services sector, such as access to advanced and detailed cyber threat intelligence as well as analysts who are skilled in dealing with cyber threat intelligence. The tests on this system are sophisticated in that they are programmed to imitate attacks that target cyber intelligence, and in this way can stay up to date with the shrewd techniques used by cybercriminals. Such testers are managed by highly skilled professionals which is beneficial in that it limits the pool of subjects that can penetrate such systems.[134]

As it has been alluded to above, there have also been directives by the EU that are still applicable to the UK. One is the Directive on Security of Network and Information Systems (NIS Directive), which was adopted by the European Parliament 2016 and placed an obligation on member states to transplant into their national legislative dispensations. This

[132] *National Cybersecurity Strategy*, 2016, 9 – 19.
[133] *National Risk Register*, 2017, 3 and 24.
[134] <https://www.crest-approved.org/schemes/cbest/index.html> on 03 February 2020.

Directive seeks to improve cybersecurity in the EU context through ensuring that member states are adequately prepared and equipped through having a NIS Authority with relevant competence as well as a CSIRT. Furthermore, that cooperation between member states and different industries in those states is fostered as a means to facilitate information sharing between member states particularly relating to threats and risks.[135]

In addition to this, the revised Payment Services Directive was published by the EU in 2016 with more comprehensive rules than its predecessor the Payment Services Directive of 2007. There are several objectives for this directive, however, making payments more secure and safer is most relevant to this study. The revised Payment Services Directive is augmented by standards relating to technical regulation; guidelines on the reporting of incidents and guidelines relating to the measures to be adopted for operational and security risks as developed by the European banking Authority together with European Central Bank. All payment service providers are accordingly required to comply with these guidelines.[136]

With respect to the institutions that have emerged, the National Cyber Security Centre was launched in 2016 in the UK. This body provides support to various critical organisations in the UK as well as the general public through the provision of appropriate incident responses to mitigate the destruction that can be triggered by such incidents. With the use of expertise in industry and academia, the body nurtures the capability of the UK to maintain secure cyberspace.[137]

Personal and physical protective advice is provided by the Centre for the Protection of National Infrastructure (CPNI), which is the national authority for this service in the UK. The CPNI is accountable to the Director-General of MI5 (part of the security service which protects the UK against threats to national security) in its functions that entail protecting national security through providing assistance in the reduction of national infrastructure

[135] < https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive> on 03 February 2020.
[136] <https://www.ecb.europa.eu/paym/intro/mip-online/2018/html/1803_revisedpsd.en.html> on 03 February 2020.
[137] <https://www.ncsc.gov.uk/section/about-ncsc/what-we-do> on 03 February 2020.

vulnerability. The National Security Strategy and National Risk Register, which have been discussed above, and the Counter-Terrorism Strategy have a significant impact on the work undertaken by the CPNI.[138]

3.5 Comparative Analysis

As it was discussed in Chapter one (1.7 research methodology), this study makes use of the descriptive research design to describe the state of affairs in the varying jurisdictions. Then a comparison is drawn between the findings on the jurisdictions with Kenya and South Africa being relevant to the African perspective and the UK presenting the international (developed perspective) which is used as a point of reference. Essentially, this constitutes a descriptive comparison which has been defined by scholars as a type of study where the occurrences of certain phenomena, and the way in which these occurrences differ in varying cases, are described.[139]

In this study, I chose three jurisdictions, namely Kenya, South Africa and the UK. The rationale for the choices lies in my intention to obtain and present findings as they apply to an African context as well as findings that are relevant to an international perspective. With this viewpoint a comparison is drawn between these two perspectives, looking at what can be borrowed from one context to the other and enhance the context that is lacking in certain respects, in this case, the African context. The focus for these jurisdictions was the interplay between e-commerce and its impact on the economies, cybercrime as well as regulatory mechanisms.

The points of comparison which I drew from looking at the different jurisdictions are as follows: the state of economic development and use of e-commerce in the jurisdiction; cybercrime statistics in each jurisdiction; the legislation developed to respond to cybercrime in the jurisdiction as well as any case law and prosecutions in terms of these legislative

[138] < https://www.cpni.gov.uk/about> on 03 February 2020.
[139] Esser F, Vliegenthart R, 'Comparative Research Methods' 2012, 12 < https://onlinelibrary.wiley.com/doi/pdf/10.1002/9781118901731.iecrm0035> on 05 February 2020.

frameworks; the institutions that have emerged together with or without legislation to address and foster cybersecurity.

In the discussion relating to e-commerce, it was uncovered that e-commerce is undoubtedly a booming industry across the world that is mainly comprised of online shopping sites, online banking and mobile payments. As such, the industry presents economic growth opportunities both in Africa and internationally. In this respect, the research suggests that the African and international perspective are similar, albeit the e-commerce industry is much larger in the UK. In other words, irrespective of the size of the industry, the potential benefits that could be brought by its activity are similar for all of the areas that were researched.

The ability to maximise these benefits is, however, stifled by various factors with cybercrime being the most relevant to this study. The statistics relevant to Kenya and South Africa illustrate that cybercrime is, and has been, on the rise at alarming rates since as early as 2012. Furthermore, that in spite of efforts to directed towards cybersecurity, cybercrime is a persistent issue. In the UK, this was a similar position until 2018, when a report indicated a decrease in cybercrime with a warning of continued vulnerability despite the decrease which was attributed to anti-virus technology.

Several technologies and systems have been developed in the UK to address the cybercrime issue. The most significant at present is the CBEST Vulnerability Testing Framework which was developed by the Bank of England in partnership with the Bank of England Sector Cyber Team in collaboration with the Council for Registered Ethical Security Testers. In addition to these institutions, policies and directives have been issued in the UK in response to cybercrime as a means to achieve a safer cyber space. When looking at the number of institutions in the UK and comparing that number to those in Kenya and South Africa, one can see a significant difference in that the UK has established more institutions than those which have been established in the two African countries. For instance, in the UK, each police department now has a unit that is committed to work, with relation to cybercrime

investigations and offender pursuits.[140] Furthermore, as mentioned in Chapter three (3.3), there are plans underway to establish specialised courts for cybercrime and other related matters.

The dispensation in Kenya and South Africa where legislation is concerned is more developed than the UK. In Kenya, legislative frameworks that speak directly to cybercrime and data protection have been promulgated between 2017 and 2019. In South Africa, the situation is similar to a bill on cybercrime published in 2017 and the data privacy regulation in 2013. In the UK, however, the most recent piece of legislation that is applicable to cyber matters was enacted in 2003. For this reason, a report has been submitted calling for revised legislation since the act on computer misuse came into force in 1990. In 2018 there was a successful prosecution in terms of this Act, as was mentioned in Chapter three (3.2). There have not been any prosecutions in Kenya and South Africa in terms of the recent legislation. However, certain sections of the Kenyan legislation have been contested in court.

3.6 Conclusion

An analysis of the regulatory environment in the United Kingdom seems to reveal that there have not been many efforts put into the framing of robust legislation to address cybercrime, and in turn promote a secure cyber environment. Instead, the focus seems to have been on the establishment of institutions to respond to the cybersecurity needs in the UK. This approach seems to be efficient, which is seen in the statistic reported on a reduction of successful cyber offences committed. Those in the legal fraternity in the UK have, however, submitted that there is a need for updated laws with the view that these developments will contribute to further victories in the fight against cybercrime.

When one views the differing as well as similar characteristics of these jurisdictions, the comparison reveals that there is a similarity in the progression of development that the African jurisdictions have taken, which is different from the practices in the UK. The most striking difference is that the efforts in the UK have been directed mainly towards institutions and less

[140] < https://saiia.org.za/research/new-bill-offers-robust-game-plan-against-cybercrime-in-south-africa/> on 05 February 2020.

on legislation wherein the African dispensations the opposite is true with legislative development being ahead and less presence of institutions seen.

Chapter Four: Conclusion and Recommendations

4.1 Introduction

This conclusion is meant to provide a detailed integration of the research findings in respect of the impact of cybercrime on e-commerce and regulatory frameworks. The findings in this research draw significantly on secondary data regarding the literature, theoretical underpinnings as well as legislation and structural developments in each jurisdiction.

In the preceding chapter, an outline of the developments that have been made has been provided. However, it has been noted that despite the developments, cybercrime continues to be on the rise and a secure cybersecurity environment is, in turn, not achieved. In this chapter I submit a conclusion and recommendations on the findings to this research.

4.2 Conclusion

The world is increasingly making use of the internet for a broad range of reasons which bring the promise of human advancement. Therefore, it becomes imperative that the spaces such as the internet are secure and measures are in place to protect users as well as to maximise the benefits that humans can reap from the use of the internet.

In the introductory chapter of this dissertation, I have described the background of e-commerce and cybercrimes and the typology of each respectively in order to provide context for the manner in which the two are related. An overview of the relevant legislation is also provided in this chapter, once again to provide context and demonstrate the interplay between regulation, e-commerce and cybercrime.

In the second chapter, I provide in-depth insights into the variables described above in the African landscape by discussing the Kenyan and the South African dispensations, respectively. The chapter begins with a discussion about e-commerce in these contexts specifically through highlighting online stores (such as Zando in South Africa) and mobile payment facilities (MPESA in Kenya) that have advanced e-commerce in both these countries. I then proceed to explore the cybercrimes statistics with the use of reports from

each country. This is done to illustrate the idea that cybercrimes and e-commerce both being reliant on the internet leads to an interplay between the two which is essentially cybercrimes acting as an inhibitor to the economic growth promised by e-commerce. Since both countries are aware of these issues, various efforts have been made to combat cybercrime. These are regulatory efforts as well as those that relate to institutions for information communications technology. From this discussion, it was noted that the development of legislation seems to be the point of focus with not as much on the structural developments. When analysing the legislative provisions that exist in the two African jurisdictions, one can make note of the ways in which they reflect the provisions in the AU convention which suggests that in that regard, both countries have executed the mandate relating to legislative development. It was also noted that the legislative developments, while a progressive step, have been contested.

Similar to its preceding chapter, chapter three provides an in-depth overview of the variables being e-commerce, cybercrime and regulation. However, the context for the discussion in the third chapter is the United Kingdom. The practices in the UK, being more developed than the two African countries, can be useful to provide insight into what has been effective in combating cybercrime. As such, I explored the legislative framework in the UK as well as the structural arrangements relating to cybersecurity and cybercrime. This examination brought to light the emergence of strategies and institutions addressing cybercrime than there have been legislative frameworks that speak directly and comprehensively to cybercrime. As a result of this, scholars and members of the legal fraternity have called for revised cybercrime laws. However, it is worth noting that even with this lack of adequate legislation, the prosecution has been made and a decrease in cybercrime has been reported.

In these chapters, I have explored the topics with a view of responding to the research questions framed in the introductory chapter. The primary question broadly asks what the impact of cybercrime on e-commerce in Kenya, South Africa and the UK is. This question is answered by the full discussions in chapters two and three in which I provide that cybercrime has impacted both regulations as well as e-commerce in the three jurisdictions.

The secondary questions require a response to what constitutes cybercrime, what constitutes e-commerce and the impact of cybercrime in each jurisdiction. Essentially these questions are a breakdown of the broad primary question and seek to respond to specific elements of the broader question. As such, the in-depth discussions into e-commerce, cybercrime and structural developments in each dispensation, respectively. From this, it can be concluded that there indeed is a relationship between cybercrime, e-commerce and regulatory frameworks. The nature of this relationship is that cybercrime is an inhibitor to the potential economic growth promised by e-commerce as it compromises the security of e-commerce users which makes it difficult for these consumers to engage in e-commerce. Further that in order to ensure the security of users, there must be robust regulatory measures in place as well as institutions to deter cybercriminals as well as to impose punitive sanctions on perpetrators of cybercrime.

4.3 Recommendations

Kenya and South Africa have both made commendable progress with the development of cybercrime and data privacy legislation. The statistics have, however, brought to light that an approach that places a focus only on legislation is not the most effective strategy. It appears that an effective strategy makes use of both legislation and institutional arrangements to respond to the issues brought by cybercrime.

In light of this, I submit that these two jurisdictions can borrow the strategies adopted in the UK, where the institutional frameworks are concerned. It is important that there are bodies to give effect to the legislative provisions, which can be done through creating a police unit for cybercrime; educating presiding officers on cyber matters; training more IT professionals as well as providing resources for the development of security systems. The establishment of units of this nature is also provided for by the African Union in the *Convention on Cybersecurity and Personal Data Protection* as has been highlighted above. It was noted that some of the difficulties relevant to the African landscape are the lack of administrative will, implementation programmes which are wanting as well as coordination of inter-governmental mandates, which I have discussed above in chapter two (2.2.2).

Based on the discussion on the different jurisdictions it can be seen that one aspect of regulation cannot be done without the other, meaning legislation should develop together with the institutions to implement what is captured in and envisioned by the legislation. In other words, it is more the enforcement aspect of regulation that needs more attention in order to achieve a holistic approach to combating cybercrime and in turn, maximise the benefits of e-commerce to the African dispensation.

References

Books

1) Comer DE, *Computer and Networks Internets with Internet Application,* Pearson Education Inc., New Jersey, 2004.
2) Wild JJ, Wild KL and Han JCY*, International Business: The challenges of globalization*, Pearson Education Inc., New Jersey, 2010.

Journal Articles

1) Brenner SW, Schwerha JJ, 'Introduction—Cybercrime: A Note on International Issues' 6(2) *Information Systems Frontiers*, 2004.
2) Cassim F, 'Addressing the Challenges posed by Cybercrime: a South African Perspective' 5(3) *Journal of commercial Law and Technology*, 2010
3) Chang W, Chung W, Chen H and Chou S, 'An International Perspective on Fighting Cybercrime' *Information Systems Frontiers,* 2003, https://link.springer.com/chapter/10.1007/3-540-44853-5_34 .
4) Cudjoe D, 'Electronic Commerce: State-Of-The-Art' 4(4) *American Journal of Intelligent Systems,* 2014, 136.
5) De Beer J *et al,* 'A Framework for Assessing Technology Hubs In Africa' 6(2), *Journal Of Intellectual Property And Entertainment Law*, 2017.
6) Halawi L, McCarthy R, 'Which Theory Applies: An Analysis of Information Systems Research' *Issues in Information Sysytems,* 7(2), 2006.
7) Jahankhani H, Al-Nemrat A, Hosseinian-Far A, 'Cybercrime Classification and Characteristics' *ReseachGate,* 2014, 157, https://www.researchgate.net/publication/280488873 , on 10 March 2019.
8) Kshetri N, 'Cybercrime and Cybersecurity in Africa' 22(2) *Journal of Global Information Technology Management*, 2019.
9) Nemat R, 'Taking a look at different types of ecommerce' (1)2 *World Applied Programming*, 2011, 101.
10) Nida T, 'The Impact of Cyberattacks on Financial Institutions' 23(2) *Journal of Internet Banking and Commerce*, 2018, 7.

11) Ndonga D, 'E-Commerce in Africa: Challenges and Solutions' 5 *African Journal of Legal Studies*, 2012.
12) Mcdermott Y, 'Conceptualizing the right to data protection in an era of Big Data' *SAGE Journals*, 2017.
13) Podgor ES, 'Cybercrime: National, Transnational or International' 50(97) *The Wayne Law Review*, 2004.
14) Raghavan AR and Parthiban L, 'The effect of cubercrime on a Bank's finances' 2(2) *International Journal of Current Research and Academic Review,* 2014.
15) Van der Merwe D, 'A Comparative Overview Of The (Sometimes Uneasy) Relationship Between Digital Information And Certain Legal Fields In South Africa And Uganda' 17(01) *Potchefstroom Electronic Law Journal,* 2014.
16) Van Niekerk B, 'An Analysis of Cyber-Incidents in South Africa' 20, *The African Journal of Information and Communication,* 2017.
17) Yar M, 'The Novelty of Cybercrime: An Assessment in Light of the Routine Activity Theory' *European Journal of Criminology (2)4,* 2005.

Other Resources

1) Akhtar I, 'Research in Social Science: Interdisciplinary Perspectives' *ResearchGate*, 2016, 73 – 74 < https://www.researchgate.net/publication/308915548_Research_Design> on 27 April 2018.
3) Bendovschi A, Cyberattacks – Trends, Patterns and Security Countermeasures, International Conference on Financial Criminology Organised by Wadham College, Oxford, 13-14 April 2015, 28-29.
4) Bowcott O, 'Cybercrime laws need urgent reform to protect UK, says report' 22 January2020 <https://www.theguardian.com/technology/2020/jan/22/cybercrime-laws-need-urgent-reform-to-protect-uk-says-report> on 04 February 2020.
5) Capital FM Kenya, 'Plight against cybercrime rife in Kenya' 02 July 2019 <https://www.capitalfm.co.ke/business/2019/07/plight-against-cybercrime-rife-in-kenya/> on 12 August 2019.

6) *Cybersecurity Readiness Report* 2017, 38.
7) Dahir AL, 'Cybercrime is costing Africa's businesses billions' *Quartz Africa*, 2018 <https://qz.com/africa/1303532/cybercrime-costs-businesses-in-kenya-south-africa-nigeria-billions/ > 05 September 2019.
8) Esser F, Vliegenthart R, 'Comparative Research Methods' 2012, 12 < https://onlinelibrary.wiley.com/doi/pdf/10.1002/9781118901731.iecrm0035> on 05 February 2020.
9) Gercke M, 'Understanding Cybercrime: phenomena, challenges and legal response' *International Telecommunications Union*, 2012, 97 <https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014_E.pdf> on 27 April 2019.
10) Gumbi D, 'Understanding the threat of cybercrime: A comparative study of cybercrime and the ICT legislative frameworks of South Africa, Kenya, India, the United States and the United Kingdom' published, University of Cape Town, Cape Town, 2018, 11.
11) Mann CL, Eckert SE and Cleeland Knight S, Global Electronic Commerce, Institute for International Economics, Washington DC, 2000, 9.
12) Muendo M, 'Kenya's new cybercrime laws open the door to privacy violations, censorship' *The Conversation*, 2018 https://theconversation.com/kenyas-new-cybercrime-law-opens-the-door-to-privacy-violations-censorship-97271 on 10 October 2019.
13) Nanfuka J, 'Sections of Kenya's Computer Misuse and Cybercrimes Act Temporarily Suspended' *CIPESA* 2018 https://cipesa.org/2018/05/sections-of-kenyas-computer-misuse-and-cybercrimes-act-2018-temporarily-suspended/ on 10 October 2019.
14) Njogore EW, 'Effects Cybercrime Related Costs on Development of Financial Innovation Products and Services: A Case Study of NIC Bank of Kenya' Jomo Kenyatta University of Agriculture and Technology, Nairobi, 2017.
15) Obeng-Adjei A, 'Analysis of Cybercrime Activity: Perceptions from a South African Financial Bank' unpublished, University of the Witwaterstrand, Johannesburg, 2017.
16) Okoth H, Ojango S, 'Kenya: Cybersecurity 2020' *ICLG.com* 2019 https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/kenya on 10 October 2019.

17) Ongeri L, 'LSK challenges the constitutionality of the Computer Misuse and Cybercrimes Act' 2018 https://www.ifree.co.ke/2018/06/lsk-challenges-constitutionality-of-the-computer-misuse-and-cybercrimes-act/ on 10 October 2019.
18) Penial BB, 'Research Design' 2017, 1 < https://www.researchgate.net/publication/308262064_Research_Design> on 27 April 2019.
19) Serianu, *Kenya Cybersecurity Reports,* 2013 – 2017.
20) Schultz CB, 'Cybercrime: An Analysis of Current Legislation in South Africa' published, University of Pretoria, Pretoria, 2016.
21) Waema TM, Ndung'u MN 'Understanding What is Happening in ICT in Kenya' Research ICT Africa, Policy Paper, 15, 2012, https://researchictafrica.net/publications/Evidence_for_ICT_Policy_Action/Policy_Paper_9_-_Understanding_what_is_happening_in_ICT_in_Kenya.pdf on 10 October 2019.
22) Wangui V, 'Petitioner challenges the Computer Misuse and Cybercrimes Act' 2018 https://www.ifree.co.ke/2018/06/lsk-challenges-constitutionality-of-the-computer-misuse-and-cybercrimes-act/ on 10 October 2019.