CYBERCRIMES IN THE KENYAN BANKING INDUSTRY: A REVIEW OF THE LEGAL FRAMEWORK ON DIGITAL EVIDENCE ADMISSIBILITY

A Dissertation submitted in Partial Fulfilment of the Requirements of the Bachelor of Laws Degree, Strathmore University Law School

By: Elsie Nyakiega

Student Number: 100030

Prepared under the supervision of

Mr. Peter Kiptanui

February 2023

Word count: 8089**(Excluding footnotes and references)**

DECLARATION

I, **ELSIE NYAKIEGA**, do hereby declare that this dissertation is my original work and that to the best of my knowledge and belief, it has not been previously, in its entirety or in part, been submitted to any other university for a degree or diploma. Other works cited or referred to are accordingly acknowledged.

Signature……*E.N.N*……

Date……19th February 2024……

This dissertation has been submitted for examination with my approval as University Supervisor:

Name……Peter Kiptanui……

Signature……

Date……19th February 2024……

DEDICATION

This research study is a dedication to the proactive approach taken by financial institutions and regulatory bodies in prioritizing the implementation of cybersecurity measures and collaboration with law enforcement agencies which contributes to the overall resilience of the banking industry against cyber threats. In addition, it recognizes the contribution of the academic and research community that continues to enrich our understanding of cybercrimes and the legal aspects surrounding digital evidence admissibility. Lastly, this paper is a dedication to the people of Kenya whose trust in the banking system forms the bedrock of economic stability and whose awareness and vigilance plays a crucial role in enabling a secure digital environment. It is my sincere hope that this research paper serves as an acknowledgement of their dedication while still encouraging them to enhance the responsiveness of Kenya's legal framework on cybercrimes and digital evidence admissibility in investigating and prosecuting such crimes occurring in the banking industry.

ACKNOWLEDGEMENT

I extend my heartfelt gratitude to my father, Mr.Patrick Njihia Nyoike, for his immense love of education and the great lengths and sacrifice he has gone to ensure I get a decent education this far. To my family and friends, I am deeply indebted to you for showing me unwavering support and believing in me even in moments when I did not believe in myself. I pay my deep sense of gratitude to my supervisor, Mr. Peter Kiptanui for his kindness, patience and helpful comments and guidance throughout this research exercise.

ABSTRACT

The research reviews the Kenyan legal framework on cybercrimes with a specific focus on the admissibility of digital evidence in court when such crimes occur in the banking industry. It then proceeds to tackle the research problem by addressing the following research objectives: First, it identifies the legal framework on cybercrimes, cybersecurity and digital evidence admissibility. It then proceeds to investigate challenges and gaps presented by the legal framework when investigating and prosecuting cybercrimes in the banking industry; finally, through a comparative study of South Africa, Malaysia and India, valuable insights are identified which Kenya can adapt to her context to alleviate the research problem. Through desktop research, the findings of this study reveal that the ubiquitous nature of the cyberspace poses great challenges in the terrestrial world when investigating and prosecuting cybercrime cases in the banking industry. It therefore proposes recommendations on the urgent need to reconsider and redraft the legal framework on digital evidence admissibility and cybercrimes to provide legal certainty. Lastly, this study is instrumental to scholars, researchers, policymakers and the Kenyan Government in reference to the research topic.

LIST OF ABBREVIATIONS

ICT	Information and Communication Technology
CBK	Central Bank of Kenya
COK	Constitution of Kenya
DPA	Data Protection Act
ODPC	Office of the Data Protection Commissioner
KICA	Kenya Information and Communications Act
CPA	Consumer Protection Act
CA	Communications Authority of Kenya
IT	Information Technology
IEA	Indian Evidence Act

LIST OF CASES

CMC Aviation v Cruisair Ltd [1978]eKLR

Ezekiel Ajwala Otin and Another v C.M Motors Ltd [2012] eKLR*; civil appeal 90 of 2008*

Weeks v *United States* (1914), The District Court of The United States

Kuruma v *Queen* (1955), The Court of Appeal for East Africa

LIST OF STATUTES AND INTERNATIONAL INSTRUMENTS

INTERNATIONAL INSTRUMENTS

Council of Europe Convention on Cybercrime, 2004

United Nations Convention against Transnational Organized Crime, 2003

The Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters, 1972

International Covenant on Civil and Political Rights, 1976

African Charter on Human and People's Rights, 1986

African Union Convention on Cyber Security and Personal Data Protection, 2014

Council of Europe Convention on Cybercrime (Budapest Convention on Cybercrime), 2001

African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention on Cyber Security), 2020

Indian Evidence Act, 1872

Information Technology Act, 2000.

KENYAN INSTRUMENTS

The Constitution of Kenya 2010

The Computer Misuse and Cybercrimes Act No.5 of 2018

The Data Protection Act No.24 of 2019

The Evidence Act, Cap 80

The Penal Code, Cap 63

The Criminal Procedure Code, Cap 75

The Data Protection Act, 2018

The Kenyan Information and Communications Act, Cap 411A

Judicature Act, Cap 8

Police and Criminal Evidence Act, 1998

CHAPTER 1: INTRODUCTION

1.1 Background

Over the years, integration of financial technology popularly known as internet banking, digital banking or e-banking has permeated explosively in today's world, amalgamating financial services and technology worldwide.[1]This has painted an impressive picture of the banking sector in the public eye as our expectations of what a bank is, and where we should find it at present is drastically different. Generally, banks are known as financial intermediaries offering a wide range of products and services fulfilling crucial liquidity functions within an economy. Aside from deposit-taking, money-lending and withdrawal services, commercial banks offer other services such as agency and advisory services entailing business risk management and performance documentation of cross-border services.[2]

E-banking is an umbrella term referring to the use of the internet by consumers to access their bank accounts through digital devices. At the basic level, internet banking is the use of mobile applications to enable customers' access to banking products and services. At an advanced level, it involves the use of Artificial Intelligence and Machine Learning to provide banking services.[3]

However, technology as we know it today is fraught with the good, the bad and the ugly. Sarcastically, the situation on the ground is laughably pitiable. Cybercrimes affect different industries yet the banking sector remains one of the worst hit industries.[4]

Due to the ever-evolving nature of cybercrimes, its definition cannot be limited to a single meaning. At best, it is considered as illegal acts perpetrated through the use of a digital device or information

---

[1] Keivani S, Khodadi M and Sourkhaouhi H,*A general view on e-banking,* Semantic Scholar,2,2012,62

[2] Mwaniki C,*How technology is transforming Kenya's banking* ,Business Daily, 7August 2016,7

[3] Delvin J, Technology and innovation in retail banking distribution, *International Journal of Bank Marketing,*4,1995,19-25

[4] Picus, key threats and cyber risks facing financial services and banking firms in 2023,3

system which could act as either the tool, target, or a combination of both.[5]Some of the common forms of cybercrimes affecting the Kenyan Banking industry includes: Malware attacks, ransomware attacks, phishing attacks, Distributed Denial of Service Attacks, identity theft and insider threats.

Despite the banking industry incurring huge financial losses, only a handful of suits end up in court as cybercrime litigation in Kenya is a slow, long and complex process requiring specialized knowledge and expertise in computer forensics investigations to produce forensically sound evidence. [6]Digital forensics is the process of obtaining, reviewing, and preserving digital evidence to ensure it is admissible in a court of law.[7] Digital forensics uses sophisticated tools and techniques to identify the source of an attack, reconstruct the timeline of events and gather evidence for legal proceedings.[8]Subsequently, the data is used to bolster the evidence of a criminal suspect, witness, or victim and to validate or invalidate claims made.[9]

In Kenya, Computer forensic investigations are facilitated by the Kenya Police under the Director of Criminal Investigations specifically at the Digital Forensic Department or by private individuals or firms. [10]However, cybersecurity is not only a matter of legal regulation but proper implementation of legal rules depends on a series of vigorous legal, technical, ethical and technological measures that

[5] Semillon R, Cano J, Cavaller V and Ruiz Cybercriminals, Cyberattacks and Cybercrime, International Journal of Computer Networks and Communications Technology,6,2016,165-176

[6] Hewling M & Saint P, Digital Forensics: the need for integration, Institute for Research in Applicable Computing, United Kingdom, 2011, 2

[7] Antwl-Boasiako A & Venter H, An Expert System for Implementing the Harmonized Model for Digital Evidence Admissibility Assessment, The International Journal of Digital Forensics and Incident Response,2

[8] Mack M, Electronic Discovery vs. Computer Forensics, *New Jersey Law Journal*,20 0ctober 2023,22

[9] Sharing Electronic Resources and Laws on Crime, UNODC Module 4: Introduction to Digital Forensics, 2013,45

[10] Kshetri N, Cybercrime and Cybersecurity in Africa, Journal of Global Information Technology Management,2019 77–81

Kenya is still struggling with.[11]

Unfortunately, Kenya's legislation on digital evidence admissibility does not nearly sufficiently address the challenges of recovering computer forensic evidence.[12] This hit-and-miss approach also places heavy evidential burden on prosecutors to produce weighty e-evidence failure to which cases are dismissed. The law's incapacity to keep up with technological developments could ultimately lead to unfavorable restrictions on the use of digital evidence in court. [13]A key objective in building and strengthening consumer trust in digital services, according to the Digital Economy Blueprint, is safeguarding the integrity of electronic and digital systems.[14]This study is a tell-tale sign that digital infrastructure development and cybersecurity cannot be divorced but instead should be developed in tandem. The study proposes practical steps on how Kenya's digital system can turn its digital ambitions into real-life achievements by identifying the challenges presented by the legal framework and possible solutions that Kenya can adapt from other jurisdictions to address the problem.

1.2 Statement of the problem

The most common legal difficulty faced by law enforcers seeking to redress cybercrimes in the banking industry in court is having digitally based evidence accepted. To guarantee admissibility in court, the evidence needs to be authentic and reliable. The second challenge is figuring out the evidentiary weight of digital data that is admitted into evidence. Digital evidence requires high

[11] Wangui P & Gaitho V, investigating extent to which cybercrime influences performance of commercial banks in Kenya, International journal of Economics, Commerce and Management,2019,491

[12] Wangui P & Gaitho V, investigating extent to which cybercrime influences performance of commercial banks in Kenya, International journal of Economics, Commerce and Management,2019,491

[13] Idris Abdi Abdullahi v Ahmed Bashane & 2 others [2018] eKLR

[14] Kenyan Ministry of Information, Communications, and Technology (2019), Digital Economy Blueprint: Powering Kenya's Transformation,2019

probative weight to be admissible in court as it is vulnerable to tampering, forgery and deletion due to its nature. It is possible to comprehend these two challenges from a technical and legal standpoint. While the law primarily addresses the first hurdle, a number of ethical, technical and technological factors are frequently taken into account to determine the second hurdle.[15] Admissibility, authentication, and weight concerns may emerge with every new type of evidence. In regards to the second hurdle, Kenya's legal framework on digital evidence barely provides legal certainty in its provisions on the scope of cybercrimes, computer forensic investigations and prosecution of such crimes in light of growing technology. The COK states that the Judiciary shall administer justice without undue regard to procedural technicalities.[16] In Kenya, justice and technicalities of law seem not to be on speaking Therefore, this paper investigates the responsiveness of the legal framework to the legal, ethical, technical and technological challenges that hinder digital evidence admissibility in court with a particular focus on cybercrime related cases in the Kenyan banking sector.

1.3 Hypotheses

1. Kenya's legal framework on digital evidence admissibility has failed to keep pace with technological advancements adapting a hit-and-miss approach when investigating and prosecuting cybercrimes in the banking industry.

1.4 Research Objectives

1. To identify the legal framework on cybercrimes and digital evidence in Kenya.
2. To investigate challenges in the legal framework that undermines successful litigation of

[15] 3 Antwl-Boasiako A, A model for Digital Evidence Admissibility Assessment, University of Pretoria,2018,54
[16] Article 159(2)(d),Constitution of Kenya(2010)

cybercrime cases in the Kenyan banking sector.

3. To identify lessons Kenya can learn from the legal framework of South Africa, Malaysia and India to successfully investigate and prosecute cybercrimes in the banking industry.

1.5 Research Questions

1. What is the legal framework on cybercrimes and digital evidence in Kenya?
2. Which challenges in the legal framework undermine successful litigation of cybercrime cases in the Kenyan banking sector?
3. Which lessons can Kenya learn from South Africa, Malaysia and India on digital evidence admissibility to support investigation and prosecution of cybercrimes in the banking industry?

1.6 Justification of the study

This study shows the need for Kenyan courts to set up an ICT division with judges and prosecutors specifically trained in cyber affairs. The judiciary needs sufficient knowledge about forensic evidence and its admissibility in order to conduct impartial, fair trials. This study also provides some background against which academics and scholars can conduct future research, as there is limited research on the problem.

1.7 Limitations

The findings of this research are limited to the banking industry and are consequently not a generalized picture of other sectors. As the banking industry in Kenya consists of a wide variety of financial institutions, research on the topic is narrowed down to Commercial Banks and the online-

banking services it provides. Owing to temporal limitations, this investigation is unable to explore the particular types of cybercrimes within the Kenyan banking sector Therefore, the study focuses on the legal framework on cybercrimes and digital evidence admissibility in the Kenyan context. Rapid changes in financial technology means the challenges facing digital evidence admissibility of such crimes in the banking industry in court is limited to the present moment as it may be hard to anticipate future challenges.

1.8 Assumptions of the study

This research is based on the belief that the Kenyan government is committed to combating crimes. There is also the supposition that the research's conclusions and findings could be beneficial and have wider application outside of Kenya. Additionally, the study makes the assumption that the Kenyan people and organizations are reasonably aware of and understand cybersecurity precautions, cyber threats and the significance of reporting cybercrime incidents.

1.9 Definition of terms

Distributed Denial of Service Attack refers to malicious internet traffic created to overwhelm the pathway of normal traffic of a targeted server, service or network or its surrounding infrastructure rendering it inaccessible.

Malware attacks is a software designed to harm a computer, server or computer network without the user's knowledge.

Ransomware attacks is a malware that encrypts a victim's data, files, devices or systems restricting access until a victim makes a ransom payment.

Identity theft is illegally using personal or financial data of another unknowing individual to commit fraud such as making unauthorized transactions or purchases.

Insider threat is a cybersecurity risk introduced by persons with legitimate access such as employees, partners, vendors, interns, suppliers or contractors with legitimate access to underlying network, data and applications who proceed to knowingly or unknowingly breach sensitive information or damage systems.

1.10 Theoretical Framework

According to Wanda Capeller, the internet has created a new, disembodied, dematerialized, and deterritorialized environment that is still largely unlike the physical world. This study weds four theories i.e. The Space Transition Theory and the Routine Activity Theory. Through these theories, the researcher investigates the nature of cybercrime the cyberspace and the role it plays in retrieval of digital evidence and admissibility in cybercrime litigation.

1.10.1 Space Transition Theory

The proponent, Jaishankar, begins by mentioning that people's actions in the cyberspace often reflect their compliance or non-compliance nature in both the physical and virtual space. [17]Stated differently, individuals who exhibit a greater aversion to crime in their physical environment are more likely to engage in cybercrimes.[18]

Secondly, he identifies that flexibility, dissociative anonymity and lack of deterrence factor in the cyberspace encourages individuals to commit cybercrimes. The theory's third section asserts that criminal activity in the cyberspace is likely to be carried over into physical space and vice versa. According to the fourth part of his theory, offenders have a way out of the cyberspace due to its dynamic spatiotemporal nature; Internet users have the liberty to visit and exit the cyberspace at will

[17] Schmalleger F & Pittaro M, Crimes of the Internet, Pearson, 322-323

[18] Arbak E, Social Status and crime, SSRN Electronic Journal,2005,5-10

and the use of anonymization techniques creates difficulty in crime attribution.

A lot of unmoderated social media platforms are great for gathering and exchanging information with like-minded individuals, but they also provide an environment where irate people can spy on, disrupt, and potentially leak confidential information. This connects to his fifth point, which says that persons in the real world are likely to band together to commit crimes in the cyberspace. Additionally, it is thought that most members of open societies are freer to express their opinions than members of closed societies, which brings us to the sixth component of the theory: members of closed societies are more likely than members of open societies to commit crimes online. Finally, the incompatibility of cyberspace norms and values with those of the physical world may give rise to cybercrimes and the challenges that follow in terms of their investigation and prosecution. Expanding the rules on traditional crimes to include e-evidence and amending existing laws to include e-evidence provisions have been the two main evidence law responses to the emergence of cybercrimes in most jurisdictions.[19] The inadmissibility of digital evidence in court can be attributed to the disregard for the distinct attributes of the virtual environment surrounding digital evidence.[20]

1.10.2 Social Learning Theory

Albert Bandura the pioneer of this theory states that people adapt behaviors by observing people and identifying the consequences of such actions. In the context of cybercrimes, most cybercrimes go unpunished and through observation of social media platforms, other individuals feel 'encouraged' to participate in other 'heinous' acts. A major appraisal of the theory is that it helps in understanding

[19] Sharing Electronic Resources and Laws on Crime, Legal Frameworks and Human Rights, *United Nations Office on Drugs and Crime*,2013,52

[20] Rutenberg I, Kiptinness S & Sugow A, Admission of Electronic Evidence: Contradictions in the Kenyan Evidence Act, *Digital Evidence and Electronic Signature Law Review,* 2021,39

the role that low conviction of cybercrimes in the banking industry plays in encouraging cybercriminals to participate in crimes as they are aware no legal action will be taken against them[21] The connection between this theory and the Study's Objectives is that the study analyzes the nature of ICT crimes in Kenya and suggests awareness raising and preventative initiatives aimed at specific social groups or communities online. Incorporating these findings into the study provides a solid theoretical foundation. By examining elements influencing cybercrimes, risk perception, and social influences, the research offers valuable insights into the factors driving cybercrimes and suggests evidence-based crime prevention strategies and policies to deal with the issue.

1.10.3 Routine Activity Theory

Marcus Felson posits that the chemistry of crime depends on the convergence of three key components in space and time: a motivated criminal, an alluring target, and the lack of capable guardianship. [22]It highlights how people's daily routines provide opportunities for criminal activity. The theory's first strength is its applicability in evaluating different kinds of cybercrimes and identifying areas cybercrime vulnerabilities.

In reference to the study's objectives this theory can be used to explain the trends and patterns of ICT crimes in Kenya. The study can help shape targeted crime prevention strategies to lessen opportunities for cybercriminals by identifying high-risk scenarios and vulnerabilities in cybersecurity.

1.10.4 Rational Choice Theory

[21] Rumjaun A & Narod F,Social Learning Theory*, Springer texts in education*,2020,85-99

[22] Lawrence E. and Marcus F. *Social Change and Crime Rate Trends: A Routine Activity Approach,* 1979-588-608

Pioneered by Ronald Clarke, he posits that the backbone of human behavior is self-interest. [23]. The basic components of the theory state that rational decisions are usually based on a cost-benefit analysis of potential risks and rewards. Choices that seem irrational to one person can be rational to another based on individual interests and any sanctions likely to be given. [24] The relationship of the Rational choice theory to the study's objectives is that it can be helpful in understanding the psychological and behavioral patterns of individuals and groups and can help in drafting and executing appropriate cybersecurity strategies in the financial industry or understanding vulnerabilities in banking operations to create cyber hygiene in the platform.

However, a downside to the theory is that it focuses on individual action which critics argue is an insufficient explanation. Another weakness is that it does not consider intuitive reasoning or instinct as a motivation behind a person's thinking process.. For example, for decisions that are a matter of life and death, one may not have the time to weigh the cost and benefits

1.11 Literature Review

Edmond Locard, the proponent of the '***Locard's Exchange Principle'*** states that according to forensic science, a criminal will bring something into the crime scene and take something with them when they leave.[25]The digital traces left is what is called *'Forensic Evidence'* which is used to trace a criminal and punish him/her. Antwl-Boasiako and Venter note that the court investigates whether the proper authorization was obtained to perform searches and seizures of digital evidence.[26] Due to

[23] Adam S, *An Inquiry into the Nature and Causes of the Wealth of Nations*,1776,200-223

[24] Raymond P, *How much do we really know about criminal deterrence,* The Journal of Criminal Law and Criminology,1973,765-824

[25] Antwl-Boasiako A & Venter H, An Expert System for Implementing the Harmonized Model for Digital Evidence Admissibility Assessment, *The International Journal of Digital Forensics and Incident Response, 2019,72-73*

[26]Goodison S, Davis R & Jackson B, Digital Evidence and the U.S Criminal Justice System: Identifying Technology

the exclusionary rule, illegally obtained evidence can be declared inadmissible in court depending on the rules of evidence of the jurisdiction.[27]

To meet the technical requirements of digital evidence admissibility, Antwl-Boasiako and Venter explain a number of requirements discussed as follows. The first step in the process of extracting, preserving, and analyzing digital evidence is to confirm the validity of forensic protocols and tools used.[28] The use of poorly tested forensic tools could lead to judges expunging digital evidence.[29]The first step in the process of extracting, preserving, and analyzing digital evidence is to confirm the validity of forensic protocols and tools used. The use of scientifically subpar laboratory facilities or improper forensic evidence storage practices could contribute to digital evidence inadmissibility. Garry and Morrissey state that the forensic report on digital evidence must be reproducible by independent third parties.

Digital forensic experts, according to Schroeder, are called upon to testify in court in two capacities. Factual testimony is needed for the first role. When the expert offers his or her opinion, which is based on their knowledge, experience, and expertise in the field, they play an additional role. According to James and Gladyshev, digital evidence is hard to extract because of the invincibility nature of the internet.[30] Through the use of anonymization techniques such as pseudonyms or proxy IP addresses, they can hide their identity in the cyberspace which makes attribution difficult. Attribution is the determination of who or what is responsible for a cybercrime.[31]Where a

---

and other needs to more effectively acquire and utilize digital evidence, *Bureau of Justice Statistics,*2015,18

[27] Cristina L, Laura A, Vazquez-Alvarez G &Vazquez- Medina R, A review of cross-border cooperation regulation for digital forensics in LATAM from the soft systems methodology, *Emerald insight,* 2022,7

[28] Article 6, *European Convention on Human rights,*4 November 1950,1995 No.2889

[29] Antwl-Boasiako A & Venter H, An Expert System for Implementing the Harmonized Model for Digital Evidence Admissibility Assessment, *The International Journal of Digital Forensics and Incident Response, 2019,*85

[30] Mason S & Seng D, Electronic Evidence, *University of London Press,*2017,422

[31] Lin H, Attribution of malicious Cyber incidents: From soup to nuts, *Columbia Journal of International*

cybercrime is reported in the banking industry, the investigation will involve assessing several devices. [32]For this reason, many investigations require several investigators working in tandem which can be time consuming and expensive.[33]

Mason and Seng's ,2017 "Electronic Evidence"[34] sheds light on the intricate legal issues surrounding digital evidence. In Kenya, the Evidence Act (as amended) recognizes the admissibility of digital evidence, but questions remain about jurisdiction and international cooperation. For instance, cybercriminals operating from outside Kenya may target Kenyan banks. Mason and Seng's work can help in understanding the legal frameworks for international cooperation in such cases, a critical aspect for Kenyan authorities.

Lin's 2016 article in the "Columbia Journal of International Affairs"[35] offers a framework for cybercrime attribution. This is particularly relevant for Kenyan banks, as cybercriminals often leverage anonymizing techniques and operate across borders. Lin's work can inform Kenyan investigators about various investigative techniques for attribution, such as analyzing network traffic and identifying malware signatures. By understanding these techniques, Kenyan authorities can improve their ability to trace cyberattacks and hold perpetrators accountable.

---

*Affairs,*2016,1

[32] Bloomberg Law, *Public Safety, Privacy and Particularity: A New Approach to Search Warrants for Digital Device,*17 June 2014

[33] Goodison S, Davis R & Jackson B, Digital Evidence and the U.S Criminal Justice System: Identifying Technology and other needs to more effectively acquire and utilize digital evidence, *Bureau of Justice Statistics,*2015,12-13

[34] S Mason and D Seng, Electronic Evidence (4th edn, University of London Press 2017).

[35] H Lin, 'Attribution of Malicious Cyber Incidents: From Soup to Nuts' (2016) 41(1) Columbia Journal of International Affairs 1.

The Bloomberg Law article 2014[36] highlights the ongoing debate regarding search warrants for digital devices. This is significant for Kenyan authorities investigating cybercrimes within the banking sector. Kenyan law enforcement needs to strike a balance between ensuring public safety and protecting the privacy of bank customers. The Bloomberg Law article can provide valuable insights into legal precedents and best practices for obtaining search warrants for digital devices in a way that respects individual privacy rights.

The fight against cybercrime in the Kenyan banking industry requires a multifaceted approach. Digital forensics plays a vital role, but legal complexities and the globalized nature of cybercrime pose significant challenges. The scholarly works discussed offer valuable frameworks and insights for Kenyan authorities to navigate these challenges and ensure effective investigations and prosecutions.

Due to varying national cybercrime laws and the rules of evidence, as well as different legal systems across nations, Brenner & Schwerha point out that multijurisdictional constraints restrict access to digital evidence. [37]Garcia and Doyle point out that requesting international assistance can be time-consuming and may not yield meaningful outcomes.[38] According to Hildebrandt, relying on digital evidence can negatively impact fairness as it does not include the suspect as a party in the investigation.[39]According to Amuchi, another conflict surrounding digital evidence admissibility in court, is that data analytics guarantees higher data privacy violations.[40]

---

[36] Bloomberg Law, 'Public Safety, Privacy and Particularity: A New Approach to Search Warrants for Digital Devices' (17 June 2014) https://www.bloomberglaw.com/ accessed 19 April 2024.

[37] Schwerha J & Brenner S, Transnational evidence gathering and local prosecution of international cybercrime, *The John Marshall journal of computer & information law,*2002,347-345

[38] United Nations Office on Drugs and Crime, *Introduction to cybercrime,*2019

[39] Hildebrandt M, Criminal Law and technology in a data-driven society, *Oxford University Press,*2014,174-197

[40] Amuchi F, Al-Nemrat A, Alazab M & Layton, Identifying cyber predators through forensic authorship analysis of chat

According to Horsman, judges in most jurisdictions operate under unclear guidelines on assessing reliable digital evidence resulting in different treatment of digital evidence.[41] Section 106B of the Evidence Act requires a certificate of authentication accompanying e-evidence, however, Section 78A states that electronic evidence is generally admissible without the certificate.[42]This is currently a source of contention in court as applying a uniform approach to digital evidence admissibility is therefore problematic.

logs, *Proceedings of the Third Cybercrime and Trustworthy Computing Workshop*,2012,28–37

[41] Horsman G, Framework reliable experimental design: A research framework to ensure dependable interpretation of digital data for digital forensics, *Computer Security,*2018, 294-306

[42] Rutenberg I, Kiptinness S & Sugow A, Admission of Electronic Evidence: Contradictions in the Kenyan Evidence Act, *Evidence and Electronic Signature Law Review,*2021,34

1.12 Research methodology

The research methodology for this study is designed to fulfill its aims and objectives through a comprehensive desktop research strategy. This involves a detailed examination of secondary sources, which encompass a range of legal provisions related to cybercrimes, the banking industry, and digital evidence within the Kenyan context.

The literature review process is conducted through an extensive analysis of various materials, including books, academic articles, newspapers, reports, and conference papers. This qualitative approach is primarily anchored on resources from Strathmore University's Online/Offline Library. In addition, a Systematic Literature Review is implemented to organize and summarize relevant research journals that are pertinent to the topic. This method involves the identification, evaluation, and interpretation of research articles that are connected to the study.

The literature of the paper is further enriched by incorporating case studies on cybercrimes within Kenya's banking sector. These case studies provide practical examples and insights, adding depth and context to the theoretical aspects of the research.

Further discussion on this topic will delve into the specific legal provisions in Kenya that address cybercrimes, and how these laws are applied within the banking sector. It will also explore the unique challenges and opportunities presented by digital evidence in cybercrime investigations. The role of the banking sector in preventing cybercrimes, and the measures they have in place to protect their digital assets and customer data, could also be examined.

Moreover, the discussion will analyze the findings of the case studies in more detail, looking at the types of cybercrimes prevalent in Kenya's banking sector, their impact, and the response strategies employed. This could provide valuable insights for policymakers, law enforcement agencies, and banking institutions in their efforts to combat cybercrimes.

Finally, the discussion will consider the implications of the research findings for future policy

development, law enforcement strategies, and cybersecurity measures within the banking sector. It will also identify gaps in the current research and suggest areas for future study. This will ensure that the research contributes to a deeper understanding of cybercrimes in Kenya's banking sector and informs effective strategies to address this critical issue.

1.13 Chapter Summary

Chapter 1

The current chapter, which is the first, is an introduction to the research topic and points out the background to the problem, the hypothesis, research objectives, research questions, justification of the study, limitations of the study, assumptions of the study, definition of terms and research methodology follow. This chapter assists the reader to understand the research problem under study.

Chapter 2

Examines Kenya's legal framework on cybercrimes, cybersecurity and digital evidence admissibility

Chapter 3

Discusses the legal, technical, ethical and technological challenges presented by the legal framework negatively impacting the investigation and prosecution of cybercrimes in the Kenyan banking industry.

Chapter 4

Is a comparative study of the legal frameworks of South Africa, Malaysia and India on provisions related to the research problem.

Chapter 5

Concludes the dissertation by stating the findings, conclusions and making appropriate recommendations to relevant authorities and on areas of future research.

VT OMNES
VNVM SINT

CHAPTER 2: KENYA'S LEGAL FRAMEWORK

2.1 Introduction

Kenya has developed several policies, laws, strategies and guidelines applicable to the research problem. Furthermore, the CAK oversees the nation's information security and conducts analysis on computer security incidences and practices through KICA.[43] The Kenya Bureau of Standards provides good practice guidelines on the design, implementation and auditing of ICT systems to enhance data protection of the data used in carrying out computer forensic investigations. It also certifies the use of (ISO/IEC 27000-SERIES) digital forensic standards.[44]

2.2 The Constitution of Kenya, 2010

Article 2 mandates the judiciary to develop the law to the greatest extent possible to fulfil its international obligations on human dignity.[45] In light of growing technology, it is the duty of policy makers and all relevant stakeholders to ensure continuous development of the legal framework on cybercrimes, cyber security and digital evidence admissibility.

According to Article 22(1), anyone can lodge proceedings in court if they believe that a fundamental freedom or right guaranteed by the Bill of Rights has been breached in one way or the other. According to Article 22(1), anyone can institute court proceedings where a fundamental freedom or right guaranteed by the Bill of Rights has been threatened, violated, or denied.[46] Article 20(3) (b) of the COK obligates the court to render interpretations of the law in a manner that most favors the application of citizens' rights.[47]Equally, Article 24(1) (e) encourages the use of less

[43] Ke-Cirt,2016

[44] KEBS, 2014

[45] Article 20, Constitution of Kenya,2010

[46] Article 22(1), Constitution of Kenya(2010)

[47] Article 20, Constitution of Kenya(2010)

restrictive means to ensure justice is rendered to all.[48] Perhaps, this is where a judge or a magistrate exercises his/her discretion on whether to admit the evidence or not in line with Article 159(2) (d).[49] If the evidence is illegally obtained, it is rejected by the court under what is called the exclusionary rule according to Article 50(4).[50] Illegally obtained evidence refers to evidence obtained through acts that go against the spirit of the constitution, statutory law and case law.[51] Which is why Article 31 on the right to privacy protects citizens from arbitrary searches which extends upon a person and his property. Therefore, forensic investigators are required to possess a search and seizure warrant before digital evidence extraction.[52]Human rights are upheld when their correlative duties are performed and are abused where there is non- performance of these correlative duties.[53]

2.3 The Kenya Information and Communications Act, 1998

According to Section 83C, the goals of the CAK are to: establish effective frameworks to lower the frequency of fraud and forgery on electronic records; provide a framework for the easier investigation and prosecution of offenders; and facilitate the effective management of vital internet resources.[54] KICA mandates the CA to develop a national agency to focus on cyber security management in the country.. Accordingly, The Kenya Computer Incident Response Team Coordination Centre is an agency established to mitigate cybersecurity threats by detecting,

[48] Article 24(1)(e), Constitution of Kenya(2010)

[49] Article 159(2)(d),Constitution of Kenya(2010)

[50] Article 50(4), Constitution of Kenya(2010)

[51] Getanda M, illegally obtained evidence: which way for Kenyan courts?, *International Journal of Liberal Arts and Social Science*,2019,2

[52] Article 31, Constitution of Kenya(2010)

[53] Mavriocola N, What is an Absolute Right? Deciphering Absoluteness in the Context of Article 3 of the European Convention on Human Rights, Human Rights Law Review,2012,79

[54] Section 83(c),*KICA*(1998)

preventing or responding to them, issuing cybersecurity advisories and enhancing cyber hygiene awareness.[55] The National KE-CIRT performs forensic examinations, various cybercrime investigations and digital evidence preparation for the prosecution of cybercrimes in criminal cases.

2.4 National ICT Policy Guidelines 2020

By regulating how data is used, distributed, analyzed or transformed into other forms, it supports computer forensics investigations and directs the orderly growth of the ICT industry. Notably, and in light of evolving technology, the policy is to be reviewed every three years, with a mid-term review occurring every five years.

2.5 The Computer Misuse and Cybercrimes Act (Act No.5 of 2018)

Computer-related offenses are covered by the Act, along with prompt and efficient detection, investigation, and prosecution of cybercrimes.[56] The National Computer and Cybercrimes Coordination Committee's procedures are outlined in Sections 4–13 of Part II of the Act.[57] It collaborates with computer incident response teams and other pertinent organizations, and it organizes the gathering and analysis of cyber threats.[58]

Sections 14–46 of Part III of the Act list particular cybercrimes and the corresponding penalties.[59]The procedural powers of cybercrime investigations are established in Part IV (sections

[55] Kohn M, Eloff J and Olivier M, *Framework for a Digital Forensic Investigation*, University of Pretoria press, 2

[56] Sang B & Sang I, Juxtaposing National Legislation with International Treaty Standards, *Commonwealth Cybercrime journal,5*

[57]Sections 4-13*,The Computer Misuse and Cybercrimes Act*(No.5 of 2018)

[58] Sang B & Sang I, Juxtaposing National Legislation with International Treaty Standards, *Commonwealth Cybercrime journal,*61

[59] Sections 14-46, *The Computer Misuse and Cybercrimes Act*(No.5 of 2018)

47–56). These powers include the ability to search for and seize computer data, intercept and retain data and examine data for evidentiary purposes.[60]The framework for cross-border cooperation of cybercrime investigations related to computer forensic investigations and prosecution of such crimes is outlined in Part V, Sections 57–65.[61]

1.6 The Consumer Protection Act, 2012

Customers of Fintech products must be protected from abusive practices that could lead to financial loss and third parties accessing their personal information without their consent.[62]The Bank is established under Article 231 of the COK.[63]Under section 4 A (1) (d) the CBK can license and supervise digital credit providers.[64]section 57(2) of the Act empowers the Bank to make regulations on credit information sharing, data protection and consumer protection.

The CBK Guidance Note on Cybersecurity Outlines efficient frameworks for risk management and cybersecurity governance for financial institutions.[65]It offers useful services to financial institutions, like consistent, independent testing and assessment of cyber threats, outsourcing guidelines, IT security awareness training and quarterly and 24-hour reporting of cybersecurity incidents. Finally, it mandates financial institutions to examine and submit their updated cybersecurity policies[66]

Central Bank of Kenya (Digital Credit Providers) Regulations, 2022

Banks are also regulated Digital Credit Providers. NCBA Bank launched M-Shwari in 2012 to provide credit facilities through mobile devices. However, M-Shwari has often been a target of Sim-

[60] Sections 47-56, *The Computer Misuse and Cybercrimes Act*(No.5 of 2018)

[61] Sections 57-65, *The Computer Misuse and Cybercrimes Act*(No.5 of 2018)

[62] Malala J, 'Consumer Law and Policy in Kenya', Journal of Consumer Policy, 2018,41

[63] Article 231,Constitution of Kenya(2010)

[64] Section 4A(1)(d), Central Bank of Kenya(Amendment)Bill,2021

[65] Article 2.1,CBK Guidance Note on Cybersecurity for the Banking sector

[66] Section 57, Central Bank of Kenya(Amendment)Bill,2021

Swap Fraud, exposing clients to unintended financial losses.[67] This act licenses and regulates digital credit providers. It forbids utilizing credit data gathered from bureaus for purposes other than those for which it was intended and disclosing credit information to unaffiliated parties. Additionally, prior to the submission or sharing of credit information, the consent of the customer must be provided. Furthermore, the consumer protection regulations found in Part VII mandate that providers set up secure systems and complaint redress channels to guarantee the privacy and security of customer information.[68] Digital credit providers are required by clause 24 to inform customers about online safety while using the internet.

[67] KICTANet, A study paper on human-centered cybersecurity: Kenyan Fintech sector,2022,14

[68] Part VII, *Central Bank of Kenya (Digital Credit Providers) Regulations*, 2022

2.7 The Data Protection Act (No.4 of 2019)

The Act gives guidance on how the banking industry should collect customers' personal data and how computer forensics investigations should be carried out to protect users' personal data while still guaranteeing admissibility in court. Section 25 of the Act states that Data needs to be handled lawfully, should adhere to cross-border transfer restrictions and data processing is in accordance with the right to privacy.[69]

The DPA requires that data subjects give their informed consent before any data is collected.[70]Therefore, forensic investigators can only retain collected personal data for the period o allowed by the Commissioner.[71] Lastly, transfer of personal data from Kenya's jurisdiction to other jurisdictions for forensic investigations is limited to evidence of sufficient data protection safeguards in foreign jurisdictions.[72]

2.8 Data Protection (*General)* Regulations, *2021*

Along with other tasks related to the Act's full implementation, the Taskforce for the Development of the Data Protection General Regulations is mandated to develop data protection laws, ensure transparency and accountability in the Act, find any gaps or inconsistencies in the Act, and propose any new policies or institutional and legal frameworks needed to carry out the Act. Additionally, it clarifies the responsibilities and duties of data processors and controller.[73]

---

[69] Section 25, Data Protection Act (2019)

[70] Section 25(d) Data Protection Act (2019)

[71] Section 25(f), *Data Protection Act* (2019)

[72] Section 25(h), *Data Protection Act* (2019)

[73] Data Protection (General) Regulations, 2021

The Data Protection (Complaints Handling and Enforcement Procedures) Regulations, 2021 and the Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021 are two of the departments that the Taskforce and the ODPC developed to help with consumer data protection. It is anticipated that the ODPC will periodically release guidelines regarding data protection. Additionally, the organization has created a Complaints Management Manual to offer direction on how to file complaints with the ODPC.

2.9 The Evidence Act (Cap 80 Laws of Kenya)

This is the main statute for both civil and criminal cases in Kenya.[74]It offers guidelines for gathering evidence prior to a trial, introducing evidence during one, and using, evaluating, and applying evidence to support or refute a claim. It also provides instructions on acceptance and display of different types of evidence.[75]

The Criminal Procedure Code (Cap 75 Laws of Kenya)

It provides for the procedure to be followed in obtaining a search and seizure warrant before obtaining digital evidence.[76]

This chapter clearly shows that Kenya has in place a competent framework on cybersecurity, cybercrimes and computer forensic investigations that supports extraction of digital evidence on paper.

---

[74] Getanda M, illegally obtained evidence: which way for Kenyan courts?, *International Journal of Liberal Arts and Social Science,*2019,1,3-4

[75] Kenya Law Reform Commission, *The Review of The Civil Procedure Act, the Evidence Act, And the Interpretation and General Provisions Act*

[76] Section 118,*The Criminal Procedure Code*(Cap 75)

CHAPTER 3: CHALLENGES PRESENTED BY THE LEGAL FRAMEWORK

3.1 Introduction

Under common law, in the case of *R v Rimmington and Goldstein* two principles are identified as the precondition of administering justice. First, unless a law is sufficiently clear and certain about what behavior is prohibited, no one should be punished under it.[77]Secondly, under the principle of *ius acceptum,* no one should be punished for any deed that was not known to be illegal at the time it was committed.[78]Lastly, legal rules need not create new crimes during interpretation of the law in a court.

3.2 Challenges

Article 159(2) (d) requires courts to administer justice without undue regard to procedural technicalities.[79] In Kenya, justice and technicalities of the law seem not to be in speaking terms especially on admissibility of digital evidence. Article 24(1) (e) encourages the use of less restrictive means to ensure justice is rendered to all through the use of the mandatory inclusion approach in regards to digital evidence.[80] However, Article 50(4) is contradictory as it applies the exclusionary rule to illegally obtained evidence, state which creates legal uncertainty.[81]

A review of Section 2 of the CMCA, indicates that the main component of computer systems is automatic data processing.[82]This is a serious flaw in the Act as it ignores technological

---

[77] Article 50(1), *Constitution of Kenya(2010)*

[78] *R v Rimmington and Goldstein* (2006),Court of Appeal

[79] Article 159(2)(d), *Constitution of Kenya* (2010)

[80] Article 24(1) (e)

[81] Article 50(4), *Constitution of Kenya (2010)*

[82] Section 2, *The Computer Misuse and Cybercrimes Act*(No.5 of 2018)

advancements like machine learning and artificial intelligence. It also repeatedly refers to '*authorized person'* as an individual responsible for detecting, investigating and prosecuting cybercrimes.[83]By failing to clearly specify such an individual, the Act grants unchecked expansion of police powers when investigating cybercrimes in the banking industry.[84]

Section 14 and 20(1) of the CMCA create offences whereby normal access by forensic investigators can be unlawful which could lead to illegally obtained evidence in court.[85]Further, the wording of the offence is legally defective as it fails to consider the mental element of such access which criminalizes innocent conduct and leads to conviction of innocent parties.[86]Additionally, the Act's Section 16(1) criminalizes unauthorized interference without tying it to the equivalent level of harm, which results in an ambiguous offense with no clear legal definition.[87]

The implication is that Kenya's penal system disregards the concepts of legal certainty and specificity, failing to distinguish between offenses that are serious and less serious.[88]The Act's section 18(1) on illegal devices and programs is worded in a way that ignores the variety of ways that technology can be used, both for legal and illegal purposes.[89] Manufacturers of digital devices, distributors, retailers, and end users are all subject to criminal liability under this standard.[90] The Cybercrimes Act disregards duplicate offenses due to its extreme zeal for criminalizing behavior,

---

[83] Sections 48-54, *The Computer Misuse and Cybercrimes Act*(No.5 of 2018)

[84] *Law Society of Kenya v Inspector General Kenya National Police Service and 3 Others* [2015] eKLR

[85] Section 14(1), *The Computer Misuse and Cybercrimes Act*(No.5 of 2018)

[86] Sang B & Sang I, Juxtaposing National Legislation with International Treaty Standards, *Commonwealth Cybercrime journal,*67

[87] *R v Rimmington and Goldstein*(2006),Court of Appeal

[88] *R v Rimmington and Goldstein* (2006),Court of Appeal

[89] Section 18(1), *The Computer Misuse and Cybercrimes Act*(No.5 of 2018

[90] Sommer, Criminalizing Hacking Tools, *Digital Investigations*, 2006, 68-72

which goes against the legal doctrine of minimal criminalization.[91]

The idea of a digital device's *proper functioning* and the capacity to attest to it are predicated on the idea that forensic investigators can quickly identify inaccuracies in e-evidence falsely provides the court with assurance on certainty.[92]The fact that the section concentrates on the device that produces such output makes it discriminatory towards certain types of e-evidence. It does not include specifics that are necessary to allow digital evidence to be admitted, such as ownership, general information about the device's hardware and software, and any recent repairs.[93] Kenya's evidence law framework does not recognize the different forms of evidence. [94] The requirement that a *responsible person* needs to sign the certificate exacerbates the aforementioned issues. It is difficult to identify this person when evidence is transferred multiple times before it is presented in court, is common with forensic investigations.[95]Without clear clarification as to who a 'responsible person' is, this requirement creates challenges in determining whether a forensic analyst is a responsible person handling digital evidence and whether such evidence is admissible in court.[96]

There is a chance that newly discovered incriminating evidence will be concealed, altered, or destroyed before a new search warrant is issued if the investigator finds it in plain sight but it is not covered by the existing one.[97] Additionally, in cases where the judge lacks knowledge about the potential risks associated with specific technologies or investigative techniques, or is not informed about the reasons behind a particular method's preference in a given case, the judge is unable to assess the level of invasiveness of the forensic technique used and the search warrant issue becomes

[91] Sections 6, 7 &10, *Evidence Act* (Cap 80 Laws of Kenya)

[92] Sections 106B(2 &4), *Evidence Act* (Cap 80 Laws of Kenya)

[93] *United States v Jackson*(1968),United States Supreme Court

[94] *Bates v Post Office Ltd Horizon*[2019]EWHC

[95] R v Edward Kirui [2010] eKLR

[96] *State v Cook*[1965],Supreme Court of New Jersey

[97] *Wisconsin v Schroeder*(1952), Supreme Court of Wisconsin

a blunt tool of procedural convenience.[98] This issue has not really been considered in Kenya's Criminal Procedure Code on search and seizure.

[98] *Njonjo Mue & another v Chairperson of Independent Electoral and Boundaries Commission & 3 others* [2017] eKLR

CHAPTER 4: COMPARATIVE STUDY

4.1 Introduction

4.2 SOUTH AFRICA

Section 1 of the country's Cybercrime Act defines financial institutions and specifically creates a provision for it unlike the Kenyan Cybercrimes Act which is a national legislation generally applicable to different sectors of the economy.[99] Subsequently, the South African law in Section 11 defines a *restricted computer system* as any data or digital device controlled by or solely utilized by a financial institution.[100]

Section 3 of the South African Act on cybercrimes provides better legal certainty than the Kenyan Act, as it clarifies what constitutes illegal interception of data.[101] This also holds true for anyone who may not have committed the initial act but is aware they are in possession of illegally obtained data.[102] Any further use or access to such data is prohibited by this clause.[103] If such information is discovered to be in the possession of someone, that person is legally guilty unless they can provide a convincing account of how the information came to be in their possession. Kenya can apply these helpful provisions to its own situation in order to provide legal certainty on unlawful possession of data in its cybercrime laws.

Interference with data or computer programs is prohibited in the South African Act in Section 5.[104] To elaborate further, the Act offers a specific definition of the components of the crime of

---

[99] Section 1, The Financial Sector Regulation Act (No. 9 of 2017)

[100] Section 239, *Constitution of the Republic of South Africa* (1996)

[101] Section 3 (2), *South African Cybercrimes Act (2021)*

[102] Section 3, *South African Cybercrimes Act (2021)*

[103] Section 3 (2), *South African Cybercrimes Act (2021)*

[104] Section 5, *South African Cybercrimes Act (2021)*

interference referring to it as acts such as erasing, altering, watering down, blocking, stopping, or hindering access to data or a computer program. The drafted definition grants courts' legal certainty in prosecuting cybercrimes occurring in the banking industry.

In terms of aggravated offenses, Section 11 of the South African Act on internet crimes specifies that it applies to Sections 3 (1),5 (1), 6 (1), or 7 (1) insofar as passwords, access codes or comparable data and devices are involved. In this case, an infringer or perpetrator is considered to have committed a crime if they knew, should have known, or had reasonable suspicion that the computer system is restricted.[105]

The sections mentioned above are a wake-up-call to Kenyan policymakers and the legislature on the need to draft clear cybercrime laws that provide legal certainty by providing clear definitions on the scope of limitation. This will greatly assist the judiciary in efficiently and effectively investigating and prosecuting cybercrimes in the banking industry.

4.3 MALAYSIA

Electronic evidence is admissible in Malaysian courts under Sections 90A, 90B, and 90C of the Malaysian Evidence Act which govern both criminal and civil proceedings. [106]On the requirement of a certificate authentication, the Act specifies that a certificate from the computer owner must be produced in order for electronic evidence to be authenticated unlike the Kenyan position which requires it to come from the forensic investigator.[107] The Malaysian position is that failure to do so makes evidence produced by computers inadmissible. Nevertheless, if the aforementioned

[105] Sections 3 (1), 5 (1), 6 (1) or 7 (1), *South African Cybercrimes Act (2021)*

[106] Mohamed A, Admissibility and Authenticity of Electronic Evidence in The Courts of Malaysia and The United Kingdom, International Journal of Law, Government and Communication,4,15,2019,121-129

[107] Bank Bamiputra Malaysia Berhad v Emas Bestari & Anor, (2014) High Court of Malaysia

individual is present at the case hearing, the certificate is not required. However, section 90C stipulates that any legal requirement pertaining to the production, admission, or proof of evidence will be superseded by sections 90A and 90B. As currently drafted, the Malaysian laws provide certainty as to the requirement of a certificate of authentication when presenting digital evidence in regards to tracing the owner as digital devices can be used by numerous people.

On search and seizure, Section 116B(2) of the Malaysian Criminal Procedure Code legitimizes illegally obtained evidence and further states that the police are permitted to access any necessary password, encryption code, decryption code, software, hardware or any other means required to collect data in a visible and legal form from a digital device.[108]This is an applaud able positon that Kenya can adapt to her context specifically in the Criminal Procedure Code where search and seizure mainly provides for collection of traditional evidence in the physical world and is extrapolated to apply to extraction of digital evidence occurring in the cyberspace.

The provision is also used to compel production of an encryption key and non-cooperation amounts to obstruction of justice subject to criminal charge.

4.4 INDIA

The admissibility of digital evidence in India is governed by the Indian Evidence Act of 1872 and the Information Technology Act of 2000 which is in line with the United Nations Obligation on International Trade Law.[109] The 1872 Act under section 64 provides for primary evidence while secondary evidence is provided for under section 65.[110] The Indian Evidence Act states that

[108] Section 1116B, Criminal Procedure Code(Amendment),(No.2 of 2012)

[109] *Gnasegaran a/l Pararajasingam v Public Prosecutor* [1997]High Court of Malaysia

[110] Section 65 A and B, *Indian Evidence Act* (1872)

obtaining a certificate is a factual requirement.[111]In the case of Shafhi Mohammad v. State of Himachal Pradesh, the divisional bench clarifies that the requirement of a certificate under Section 64B (4), being procedural, can be relaxed in circumstances where the interest of justice would be for the electronic device to be produced by a party that does not own that device.[112] This provision provides for legal certainty as to the circumstances surrounding production of a certificate of authentication.

For instance, a document from a Google website can be certified by any authorized individual who has legal access to the document in electronic format instead of just a Google server administrator which is a source of contention in Kenya's legal framework on lack of specification on who an 'authorized person' is. [113]Further, according to IEA, digital evidence must be produced by a content viewer in accordance with Section 65B of the act, which draws a distinction between content owners and viewers. A bank statement, for instance, has the official bank manager as the content owner, who is regarded as the authority in the field and is able to provide a printout of the statement as proof of ownership. This another distinction offered by IEA on the requirements of an 'authorized person' which Kenya can include to her Evidence laws.

Section 65B(2) specifies the 'regular activities' of a digital device. First and foremost, it states that computer output is accepted only where the computer is frequently used to store or process information on activities normally done by the 'legally controlling person'.[114] Secondly, during that particular period, information of the type contained or extracted from the electronic record has been regularly entered into the computer in the normal course of said activities. Third, in regards to

---

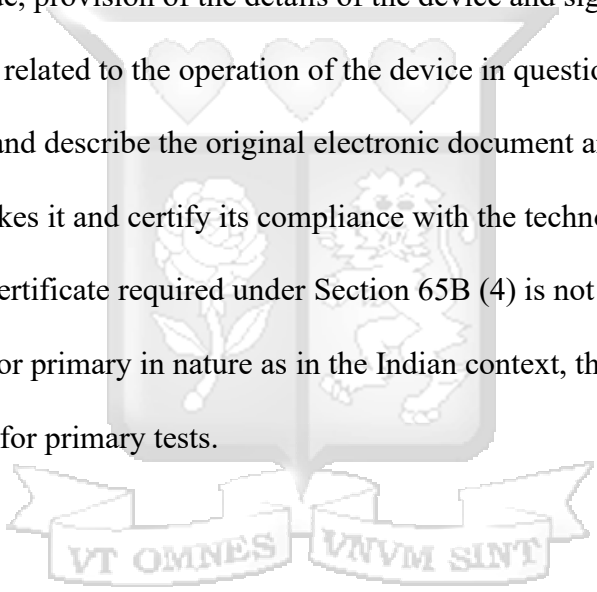
[111] Section 65B(4), *Indian Evidence Act* (1872)

[112] *Shafhi Mohammad v. Himachal Pradesh state*, [2018], Supreme Court of India

[113] Sections 48-54, *The Computer Misuse and Cybercrimes Act*(No.5 of 2018)

[114] Section 65B(1) *The Indian Evidence Act*, 1872

'*proper functioning'*, throughout the material/physical part of the mentioned period, it is a requirement under the Indian law that the computer was functioning correctly. If it was inoperative during that period or a part of it, for digital evidence to be admissible, it needs to be operative in respect to electronic filing or accuracy of its content. [115]These are applaud able provisions that Kenya can adapt to her context to provide legal certainty to its provisions on digital evidence. Regarding an '*authorized person'* issuing a certificate and its content, the requirements stipulated in the IEA include identification of the electronic file that contains the declaration, description of how the electronic record is made, provision of the details of the device and signature of a person holding an official position related to the operation of the device in question. [116]The certificate needs to uniquely identify and describe the original electronic document and how it is made, describe the device that makes it and certify its compliance with the technological conditions set out in Section 65B(2).[117] The certificate required under Section 65B (4) is not necessary if the original document is self-produced or primary in nature as in the Indian context, the certificate is necessary for secondary tests and not for primary tests.



[115] Naman J & Reddy S, Admissibility of Digital Evidence in India: An Overview, *Alliance School of Law,*2020,11

[116] Anvar P.V v Basheer P.K [2014] *Supreme Court of India*

[117] Section 65B (4), *The Indian Evidence Act*, 1872

CHAPTER 5: FINDINGS, CONCLUSIONS AND RECOMMENDATIONS

5.1 Findings

Kenya has a legal framework in place to address cybersecurity, cybercrimes, and computer forensics. This framework includes the Constitution of Kenya,2010, the Kenya Information and Communications Act, the National ICT Policy Guidelines, the Computer Misuse and Cybercrimes Act, the Consumer Protection Act, the Central Bank of Kenya Act, the Central Bank of Kenya Guidance Note on Cybersecurity for the Banking Sector, the Data Protection Act, and the Evidence Act.

Challenges

The Kenyan legal framework has some challenges that undermine successful litigation of cybercrime cases in the banking sector. There are contradictions between Article 159(2)(d) requiring administration of justice without technicalities and Article 50(4) on the exclusionary rule. The Computer Misuse and Cybercrimes Act is criticized for not being clear and specific, failing to distinguish between serious and less serious offenses, and not providing clear definitions for digital evidence. The Evidence Act does not recognize different forms of digital evidence and has ambiguous requirements for a certificate of authentication. Search and seizure procedures may not be adequate for collecting digital evidence.

Lessons Learned from Other Countries

South Africa's Cybercrimes Act offers a clearer definition of illegal interception of data and possession of illegally obtained data. The Act also provides a specific definition of data interference. Malaysia's Electronic Evidence Act has clearer specification on certificate authentication compared to Kenya. Their Criminal Procedure Code also has a provision to compel

production of an encryption key. India's Information Technology Act provides legal certainty regarding the certificate of authentication by specifying who can issue it. Their Evidence Act also offers a clearer definition of "regular activities" of a digital device and the requirements for an "authorized person" issuing a certificate.

5.2 Conclusion

This study underscores the importance of adopting a tailored approach to cybercrime litigation, as a one-size-fits-all strategy proves to be problematic, outdated, and ineffective. The research not only sheds light on the issue but also lays a robust foundation for future academic investigations and policy development aimed at fostering a secure and resilient digital ecosystem in Kenya.

The ongoing efforts to protect Kenya's digital infrastructure from escalating threats can draw upon the practical and evidence-based recommendations provided in this study. Consequently, this paper posits that the current methodology employed by Kenya's judiciary in the investigation and prosecution of cybercrimes is largely unsuitable and ineffective.

The practice of entrusting cybercrime litigation to individuals with limited expertise in the field of Information and Communication Technology (ICT) raises serious concerns. Therefore, it is crucial to ensure that those handling such cases are adequately equipped with the necessary knowledge and skills. This will enhance the effectiveness of the judicial process in dealing with cybercrimes and contribute to the overall cybersecurity landscape in Kenya.

5.3 Recommendations

In order to equip citizens with knowledge about cybercrimes and their various forms, it is imperative for the Ministry of ICT to initiate public awareness campaigns and sensitization programs. Moreover, collaboration with educational institutions, media outlets, and community leaders is essential to enhance the reach of these awareness efforts.

Promoting active participation of the youth in the legislative process and implementation of

cybercrime laws and digital evidence laws is also crucial. Addressing root causes such as youth empowerment and unemployment through initiatives aimed at skill development can equip young people with the necessary resources to maintain ethical conduct online.

The government should allocate sufficient funds for the training and capacity building of law enforcement personnel to enhance their skills in investigating cybercrimes. Adequate funding for ICT regulatory organizations is also necessary. The development of a coordinated strategy to combat cybercrimes, particularly in the banking sector, calls for increased collaboration among government agencies, businesses, civil society organizations, and international partners.

This research underscores the need for a case-specific approach in cybercrime litigation, as a standardized approach proves to be problematic, outdated, and ineffective. The study not only provides valuable insights but also lays a robust foundation for future academic research and policy development aimed at creating a secure and resilient digital environment in Kenya. The ongoing efforts to protect Kenya's digital landscape from escalating threats can be guided by the practical and empirically supported recommendations provided in this study.

The paper asserts that the current approach adopted by Kenya's judiciary in investigating and prosecuting cybercrimes is largely unsuitable and ineffective. Entrusting cybercrime litigation to individuals with limited expertise in the field of ICT raises serious concerns.

Reviewing digital evidence and cybersecurity policies will help eliminate redundant clauses, clearly define the boundaries of offenses, and provide a clearer understanding of the objective and subjective components of cybercrimes. Many of the existing provisions conflict with the 2015 Kenyan Sentencing Guidelines due to overlapping or nearly identical clauses. The majority of penalties under Kenya's legal framework do not differentiate between severe and less serious forms of harm, resulting in comparable punishments for minor and significant harm caused by cyber-conduct.

REFERENCES

M Akech, Administrative Law (Strathmore University Press, 2016.

J Ambani and K Mbondenyi, The New Constitutional Law in Kenya: Principles, Government and Human Rights, Law Africa, 2012.

Bloomberg Law, 'Public Safety, Privacy and Particularity: A New Approach to Search Warrants for Digital Devices' , 17 June, 2014, https://www.bloomberglaw.com/ accessed 19 April 2024.

L Franceschi and PLO Lumumba, The Constitution of Kenya: a Commentary (2nd edn, Strathmore University Press, 2019.

H Lin, 'Attribution of Malicious Cyber Incidents: From Soup to Nuts', 2016, 41(1) Columbia Journal of International Affairs 1.

PLO Lumumba, K Mbondenyi and S Odero, The Constitution of Kenya: Contemporary Readings, Law Africa, 2013.

K Mbobu, The Law and Practice of Evidence in Kenya, Law Africa, 2011.

S Mason and D Seng, Electronic Evidence, 4th edn, University of London Press, 2017.