EFFICACY OF THE CYBERSECURITY LEGAL FRAMEWORK IN ADDRESSING CYBERCRIME: A FOCUS ON KENYA

UNIVERSITY OF NAIROBI

MASTER OF LAWS

ELIZABETH MOSA AGINA

G62/38188/2020

A Research Project Submitted to the University of Nairobi Law School in Partial Fulfillment of the requirements for the Master of Laws (LL.M) Degree Program.

November, 2022

DECLARATION

I, **ELIZABETH MOSA AGINA,** do hereby declare that this thesis is my original work and has not been submitted and is not currently being submitted by any other university.

…… ….……28/04/22…….

ELIZABETH MOSA AGINA **DATE**

G62/38188/2020

This research paper has been submitted for examinations with my approval as University Supervisor

….……28/04/22…….

DR. CONSTANCE WANGECHI GIKONYO **DATE**

DEDICATION

It is my sincere hope that this work will contribute to policy interventions and shall enhance awareness on cybercrime in Kenya and the available avenues to combat it. I dedicate this paper to my family and the industrious people of the Republic of Kenya who are deserving of protection against violation of their rights while using the cyberspace.

ACKNOWLEDGEMENTS

The preparation and completion of this paper and my studies is a testament of immense support received from different stakeholders in my personal, academic and professional life. At the onset I appreciate with sincere gratitude the overall guidance and tutelage of my supervisor Dr. Constance Wangechi Gikonyo whose professional support made the completion of this paper a reality.

My parents, Israel and Etheltruda, the driving force beneath my academic wings. I am truly indebted to you for your unending emotional, moral and financial support throughout my academic journey. Your reassurance on the difficult days and joyous claps on the successful days kept me going, thank you.

To my siblings; Cheguevara, Louis, Frank, Peres and nephew Hawi, your constant enquiries on my academic progress renewed my zeal to conquer this quest, I salute you. To Scovia, thank you for bringing Teko on those busy and tiresome days, it was a source of great comfort.

The gracious support of employer cannot go unnoticed. The indulgence during the entire period of my studies is appreciated with deep gratitude. My friends Nelly, Mwende, Walter, Dan, Brian, Roy and Ivor, your cheerleading through this entire course is immensely appreciated.

Most importantly, I return all glory and honour to Jehovah God who sustained me during this entire period, through the difficult health experiences upto the fruitful completion of my studies. Truly, you renewed my strength and made all things beautiful. Amen.

LIST OF CASES

Bloggers Association of Kenya (Bake) v Attorney General & 5 others [2018] eKLR.

Senate of the Republic of Kenya & 4 others vs. Speaker of the National Assembly & another; Attorney General & 7 others (interested parties) [2020]eKLR.

Speaker of the National Assembly & another v Senate & 12 others (Civil Appeal E084 of 2021) [2021] KECA 282 (KLR) (19 November 2021).

LIST OF STATUTES

Computer Misuse and Cybercrimes Act, 2018.

Data Protection Act, 2019 (DPA).

Kenya Information and Communications Act, 1998.

Mutual Legal Assistance Act, 2011.

Prevention of Terrorism Act, 2012.

The Constitution of Kenya, 2010.

LIST OF INTERNATIONAL INSTRUMENTS

African Union Convention on Cybersecurity and Personal Data Protection (AUCCPDP).

Convention on Cybercrime, ETS No.185.

ABBREVIATIONS

AUCCPDP- African Union Convention on Cybersecurity and Personal Data Protection.

CMCA- The Computer Misuse and Cybercrimes Act, 2018.

CoC- The Convention on Cybercrime.

DDOS- Distributed Denial of Service.

DPA- The Data Protection Act, 2019.

ICT- Information Communication and Technology.

IFMIS- Integrated Financial Management Information System.

KICA- Kenya Information and Communication Act, 1998.

KRA- Kenya Revenue Authority.

KUCCPS- The Kenya University and Colleges Central Placement Service.

National KE-CIRT/CC-National Kenya Computer Incident Response Team Coordination Centre.

NCCCC- National Computer and Cybercrimes Co-ordination Committee.

NEMIS- The National Education Management Information System

ODPC- The Office of the Data Protection Commissioner.

SCP- Situational Crime Prevention.

TABLE OF CONTENTS

ABSTRACT

Internet access has considerably increased globally and in Kenya over the last decade. The widened internet reach catalysed the shift of service provision to the cyberspace. Government services (education, human resource, tax administration and procurement); financial services (mobile banking and saving platforms like M-shwari) among other sectors have embraced utilising the internet and Information, Communication and Technology in conducting their business. Individuals have similarly embraced and moved to the cyberspace to engage socially and economically with others through social media platforms and other applications for different services such as transport and food delivery (Uber, Bolt, Glovo and Uber Eats).

The onset of the unprecedented Covi-19 pandemic also provided a unique opportunity for other services to shift from manual systems to digital based systems or online service delivery. To mitigate the spread of the deadly virus, predominantly manual based institutions (such as the judiciary and learning institutions), organisations and business enterprises shifted their service delivery to the cyberspace. These resultantly introduced virtual hearings and learning as well as remote working and online shopping. Increase in internet access and use of ICT also had a corresponding effect on cybercrime which also substantially increased. It was observed that whereas the State enacted legislation and established institutions to combat cybercrime, cyber threat incidents were on the rise.

In view of the growing security and economic concerns tied to cybercrime, the study reviews the existing Cybersecurity regulatory and institutional framework in Kenya to assess its impact in addressing cybercrime. This paper will also interrogate the research questions in the study. The researcher utilised doctrinal legal research which was best suited owing to the security and liability concerns that would limit disclosure by organisations and institutions on their vulnerabilities to cyber threats. The study established that an increase in use of the internet and ICT resulted in a corresponding increase in prevalence of cybercrime which continued to persist despite existence of a legal and institutional framework on cybercrime. Resultantly, it was established that lack of awareness, poor cyber hygiene and limited expertise in detection and investigation of cybercrimes contributed to the prevalence rate of cybercrime.

CHAPTER ONE: INTRODUCTION

1.0 Background of the Study

Advancing information, communication technology and its use has been on the rise globally and regionally over the last decade. This is evidenced by an increased integration of Information Communication and Technology (ICT) and the internet into existing business models[1]. Social and economic development in some economies has also been attributed to the use of the internet and reliance on ICT[2]. Service provision in different sectors spanning from education, health and finance have largely integrated the use of ICT and the internet to their business models[3].

Kenya like other countries globally has also automated to improve service delivery by introducing e-government services. The launch of e-citizen platform by the Ministry of Interior and National Coordination has for instance ben instrumental in supporting access to government services, which was a departure from the previous model where services were only accessible at the physical offices of the respective State Agencies.

Presently, several services are now available on the platform, this includes; registration and renewal of driving licenses, registration of business names or companies, application for marriage certificates, application for birth certificates as well as registration and renewal of passports. The adaptation of internet and ICT has also been replicated in the Government's tax administration service. This has been achieved through introduction of the iTax platform which is administered by the Kenya Revenue Authority (KRA).

[1] Enrico Calandro and Nils Berglund, 'Unpacking Cyber-Capacity Building in Shaping Cyberspace Governance: the SADC case' (GIGAnet Conference Paper, annual symposium, Berlin 2019).
[2] Communication Authority of Kenya (2020), *20 years of Kenya's ICT Progress* Annual report 2019-2020.
[3] Ibid.

The iTax platform enables its users to access tax related services online at the touch of a button. This being an improvement from the previous service model where services were solely accessed manually and clients had to lodge their tax returns and seek other tax related services at the KRA physical offices. The iTax platform provides a mechanism for its users to lodge tax objections, apply for waivers on penalties and interest as well as requisition for compliance certificates online among other tax related services.[4]

The National Treasury has also jumped on board with automation by creating the Integrated Financial Management Information System (IFMIS). IFMIS is an online system of managing public finance with an array of services including planning, financial reporting and budget execution.[5] It conveniently connects all government ministries, agencies and departments through a network into a single public finance management system accessible online. It has also enabled automation of the government procurement process which was previously manual and could easily be manipulated. The IFMIS system, first launched in 2003, has been lauded for its role in improving transparency and accountability in public finance management in line with our principles of governance and national values[6].

The integration of ICT and the internet to existing service models in finance, tax administration and government services are just the tip of the iceberg on shifting business models in the Kenyan

[4] Dennis Onsongo, 'How KRA can make the most of its iTax platform,' *The Business Daily* (Nairobi, 16 June 2019).
[5] The National Treasury, 'IFMIS Department' (*The National Treasury*, June 2022) <https://www.treasury.go.ke/ifmis/#:~:text=One%20of%20the%20PFM%20reforms,at%20enhancing%20accountability%20and%20transparency.>accessed 30 October 2022.
[6] Constitution of Kenya, 2010 article 10(2) (c).

market. Notably, several benefits have been credited to the use of ICT and the internet in service delivery. The KRA iTax platform for instance has been reported to have improved compliance and broadened the tax base. It has also enhanced tax revenue collection by Kenya Shillings 115 billion as recorded in the 2016/2017 financial year when it was fully operational[7].

The IFMIS system on the other hand has improved accountability and transparency in public finance management through introduction of proper financial controls[8].Similar improvements have been noted for the e-Citizen platform which has simplified access to government services by providing step by step guidance to access services remotely. Individuals using the e-Citizen platform can now conveniently apply for registration of their marriages, apply for birth certificates and register business online without the mandatory need to visit physical government offices for the same service.

While the benefits associated with automation of services are alluring, it cannot be gainsaid that they come with their share of negatives which similarly impact on the very people they aim to serve. Integration of internet and ICT in service delivery has exposed government online based platforms to wider reach by anyone with internet access, including cyber criminals. The automated platforms have also become open targets for manipulation through crimes perpetuated in the cyberspace.

[7] Dennis Onsongo (n 4).
[8] ICPAK, 'The benefits, challenges and way forward of IFMIS in Kenya' (IPSAS Workshop, 27th-28th June 2017, Merica Hotel, Nakuru) 16.

It has been estimated that the Kenyan economy has lost up to $210 million to cybercrime. The Kenya Revenue Authority for instance has been a victim of alleged theft of 39 million US dollars through electronic fraud[9] following a breach of its computer systems[10]. The National Treasury IFMIS system has equally been a victim of cyber-attacks which resulted in website defacement of the informational page[11].[12]In view of the foregoing, it is has become evident that while automation of services has achieved significant benefits, it has also introduced challenges that substantially increase risk of exposure to cyber insecurity in the form of cybercrimes[13].

Consequentially, any undermining of the prevalence of cyber insecurity through cybercrime would be foolhardy not only to the safety of users of the various services and platforms but to the economy as well. To navigate the shift to the unchartered cyberspace and its new found challenges it became necessary to develop a legal framework to not only regulate conduct in the cyberspace but to also regulate the use of ICT and the internet, safeguard cyber security and curb cybercrime.

While there is no international instrument safeguarding cyber security, some regions have developed conventions to address cybercrime which can be relied on as a baseline.[14] The Council of Europe has a convention,[15] which defines cybercrime offenses and incentivises global

[9] BBC News, 'Kenya Revenue Authority 'Lost $39m to hacker,' *BBC News* (22 March 2017) 4.
[10] Paul Ogemba, 'Man charged with hacking KRA and causing Kenya shillings 4 Billion loss*' The Standard* (Nairobi, 22 March 2017) 6.
[11] Benjamin Muriuki, 'IFMIS safe and secure, says gov't after 18 websites reported hacked' *Citizen Digital* (Nairobi, 3 June 2019) 11.
[12] Nir Kshetri, 'Cybercrime and cybersecurity in Africa,' (2019) 22 (2) Journal of Global Information Technology Management 77, 81.
[13] Valery O. Lutta and John Obiri, 'Cyber Crime a Rising Threat for Internet – Based Businesses in Western Region, Kenya' (2015) 6 (3) International Journal of Scientific and Engineering Research 317, 320.
[14] Mittal, Sandeep, and Prof Sharma, 'A review of international legal framework to combat cybercrime' (2017) International Journal of Advanced Research in Computer Science 2.
[15]Convention on Cybercrime, ETS No.185, article 2-12.

collaboration.[16] Similarly, the African Union has a convention which establishes a regional regulatory regime for the protection of personal data protection whilst also mandating Member States to enact legislation against cybercrime.[17]

Domestically, Kenya has enacted three laws which regulate the ICT sector while regulating interactions over the cyberspace to ensure rights and fundamental freedoms.[18] Kenya Information and Communications Act, 1998[19] is the first legislation defining cyber security[20] in Kenya. The Act was enacted to regulate the communications and electronic commerce sectors in the advent of the internet and computer technologies in Kenya. It creates the Kenya Communications Authority, whose obligation encompasses safeguarding security in the cyberspace through ensuring use of dependable digital records [21] and designing frameworks to reduce fraud in e- commerce and other digital payments.[22] The Kenya Communication Authority is also credited with making a framework for examining and prosecuting cybercrimes.[23]

In 2018, the Computer Misuse and Cybercrimes Act (CMCA) was enacted in response to Kenya's progressing cyberspace. The Act attempted to stop the unauthorized use of computer networks,[24] protect the right to privacy, improve access to information, encourage free expression,[25] as well as facilitate prosecution of related offenses.[26] It sought to prevent illegal use of computer systems and

[16] Ibid 23.
[17] African Union Convention on Cybersecurity and Personal Data Protection (AUCCPDP), article 25(1).
[18] Constitution of Kenya, 2010 Article 31 and 35.
[19] Kenya Information and Communications Act, 1998.
[20] Ibid, s 2(1).
[21] Ibid, s 83C (1) (a).
[22] Ibid, s 83C (1) (f).
[23] Ibid, s 83C (1) (h).
[24] Computer Misuse and Cybercrimes Act, 2018 (CMCA), s 3(b).
[25] Ibid, s 3(d).
[26] Ibid, s 3(c).

protect the right to privacy.[27]It also sought to make cybercrime detection, investigation, prosecution, and punishment easier.[28]

It also distinguishes different cybercrime offences and stipulates charges and fines payable when one is found guilty of the said offence. It also prescribes modes of undertaking investigations. Further, it provides a mechanism for international co-operation noting that cybercrime is not limited to physical jurisdictional boundaries.

The Data Protection Act, 2019 (DPA) is perhaps the most recent legislation enacted to complement the established cyber security legal framework.[29] It protects the processing of personal data[30]. The Act outlines both legal and institutional ways [31]to protect individuals' privacy in accordance with the Constitution.[32]Its focus is on protecting personal information processing to improve realization of the right to privacy in family or private affairs and related communication.

In spite of the existing cybersecurity legal framework, cybercrime in Kenya continues to evolve and permeate in different sectors which utilize automated services. This study will therefore seek to assess the existing cybersecurity legal framework with a view to determining its impact in addressing cybercrimes in Kenya as well as propose mechanisms to curb and minimize cybercrime.

[27] Ibid, s 6(1) (d).
[28] Ibid, s 6(1) (j).
[29] Data Protection Act, 2019 (DPA), s 3(a).
[30] Ibid, s 3(d).
[31] Ibid, s 3(c).
[32] Constitution of Kenya, 2010 article 31 (c) and (d).

1.1 Statement of the Problem

Reliance on use of internet and ICT in carrying out day to day activities such as banking, communication and access to government services has greatly improved service delivery. Services are now easily and conveniently accessed remotely at the touch of a button. This is devoid of the challenges associated with analogue service delivery which was time consuming, required physical presence and was associated with long queues.

While the shift to the cyberspace has improved service delivery in various sectors, it has also exposed service providers and their consumers to cyber threats arising from security breaches. Some of the cyber threats associated with illegal intrusions have resulted in unauthorized access to institutional and client information and commission of cybercrimes including online fraud, impersonation and forgery.

Cybercrime linked to the aforementioned cyber threats has caused significant effects in the economy culminating in losses in various sectors including the Banking industry which has been exposed through their online banking platforms[33]. The effects have also span to other service providers using automated services such as the Government and telecommunication institutions which have shifted to mobile and internet banking.[34]

Whereas significant legal and policy interventions have been put in place to safeguard cybersecurity, cybercrime continues to be prevalent. Between January and March of 2021 for

[33] Munguti Richard, 'JKUAT students charged with hacking bank, stealing millions' *Daily Nation* (Nairobi, 27 October 2020) 5.
[34] Olingo Allan, 'Two Kenyan banks lose $ 0.86 million to hackers in a month' *The East African* (Nairobi, 14 July 2018) 2.

instance investigation of cases relating to online fraud increased with a variation of 96.9%.from those investigated between a similar time frame of three months between October and December 2020[35].

A similar increase was noted with regard to digital investigation requests for cybercrime which increased by 33.0% over the same comparative period[36]. The increase in cybercrime over the period may be attributed to the continued shift to digital products and online platforms especially at the onset of the Covid-19 pandemic which necessitated shifting of business models to ensure continuity.

While Kenya benefits from having a legal framework addressing cybersecurity broadly with a reference to cybercrime, it appears the framework has neither adequately deterred cybercrime nor reduced the allure to commit it. This study therefore seeks to address the underlying challenges contributing to prevalence of cybercrime in Kenya despite the existence of a cybersecurity legal framework.

1.2 Statement of Objectives

The study seeks to assess the efficacy of the cybersecurity legal framework in addressing cybercrime in Kenya. The study will therefore focus on the following key objectives:

1. To highlight the status of cybercrime in Kenya.
2. To analyse the existing cyber security legal framework addressing cybercrime in Kenya.

[35] Communications Authority of Kenya (2021), Third Quarter Sector Statistics Report for the Financial Year 2020/2021.
[36] Ibid.

3. To evaluate the effectiveness of the cybersecurity legal framework in addressing cybercrime in Kenya.

1.3 Research Questions

The following research questions will be addressed by this research:

1. What is the status of cybercrime in Kenya?
2. What is the existing cybersecurity legal framework addressing cybercrime in Kenya?
3. How effective is the cyber security legal framework in addressing cybercrimes in Kenya?

1.4 Hypotheses

The researcher's study is informed by three hypotheses:

1. Increased automation of services and the proliferation of the use of ICT and the internet in Kenya has enhanced access to services for everyone while also exposing them to cybercrime.
2. Cybercrime has become more prevalent in Kenya following increased use of information communication and technology (ICT) and automation of services.
3. Cybercrime continues to be prevalent in Kenya despite existence of a cybersecurity legal framework addressing cybercrime.

1.5 Justification of the Study

Several sectors have incrementally shifted their service delivery to the cyberspace to keep up with global trends and enhance their reach to the available client base. The Banking sector for example has gradually embraced e-banking. Bank customers can now transact their business online without

the need to physically visit banking halls or Automated Teller Machines (ATMs). This is an improvement in the mode of doing business to the delight of customers. In the same breadth, e-banking has exposed both users and banking institutions to cybercrimes as evidenced by increased reports of cyber-attacks affecting ATMs through malwares between 2019 and 2020[37].

The novel Covid-19 virus further catalysed the inevitable shift to automation with many institutions migrating their services online. Institutions that offered physical services pre-Covid 19 were now able to maintain service delivery in light of the pandemic as mitigation measures limiting physical contact were implemented.

The Communications Authority of Kenya for instance introduced three short codes and USSD codes to enable the public access services related to Covid-19. The codes provided an avenue for members of the public and other stakeholders to seek emergency response, mental and psychological support, lodge complaints regarding government's response to the pandemic while also receiving information on Covid-19[38]. The automation shift was also adopted by the Kenyan Judiciary and education institutions in the wake of Covid-19. Both entities utilized online mechanisms including virtual court sessions and virtual classes as mitigation measures to reduce physical interaction while safeguarding access to education and administration of justice despite uncertain times.

[37] Serianu (2020), *Local Perspective on Data Protection and Privacy Laws: Insights from African SMEs* Africa Cybersecurity Report Kenya, 2019/2020.
[38] Communication Authority of Kenya (2020), *20 years of Kenya's ICT Progress* Annual report 2019-2020.

In the course of 2020 as the spread of Covid-19 was nearing its peak for the first wave in Kenya, the shift to use of internet and ICT to conduct business and work remotely also increased in other sectors with a reported 50% increase in unsecured remote connection[39].As a result of the shift in business models and adaptation of remote working for several institutions as depicted above, there was a significant increase in users of the cyber space. The new users inadvertently then became susceptible victims to cybercrime which increased over the said period.

Under the guise of providing information on Covid-19, cyber criminals have explored vulnerabilities and are using a variety of cyber-attacks to steal user information and defraud the unsuspecting recipients[40]. This is despite existence of a cybersecurity legal framework which ought to safeguard legislative protections relating to access to information, privacy and prescribe punishments for cybercrime offences.

In spite of the foregoing challenges, new entrants to the cyberspace and all users are deserving of protection under the cybersecurity legal framework. It has therefore become necessary now more than ever to interrogate the adequacy of the existing cybersecurity legal framework in addressing cybercrime in Kenya. This is especially significant due to the increased reliance on ICT and the internet by the Government, businesses in diverse sectors and members of the public.

This study will therefore highlight the effectiveness of the current cybersecurity legal framework in addressing cybercrime. It will also enable the researcher to outline any challenges in the fight against cybercrime in Kenya including those that may be linked to the current cybersecurity legal

[39] Ibid.
[40] Communications Authority of Kenya (2020), *National Cyber Security Report for The Period January-March 2020*.

framework. The study will also propose recommendations to enrich the existing cybersecurity legal framework with a view to reducing cybercrime and enhancing awareness on cybercrime and cybersecurity in general.

At the conclusion of this study, it is expected that all actors in the cyberspace both locally and internationally will utilise the research findings to safeguard themselves against cybercrime and the findings will provide the hallmark for an effective cybersecurity legal framework.

1.6 Theoretical Framework

The study relies on two theories; the deterrence theory and the situational crime prevention (SCP) theory. These theories are significant owing to their background in addressing crime in the physical realm and their applicability to crimes committed in the cyberspace.

1.6.1 Deterrence Theory

The Deterrence theory gained prominence in the early writings of Ceasare Beccaria and Jeremy Bentham in the late 1700s[41]. Both theorists posited that societies required restrictions on permissible conduct to discourage people from harming others in their individual pursuit of happiness and satisfaction[42]. They proposed imposition of punishments for certain acts so as to deter the populace from committing the said acts out of the fear of being subjected to the punitive punishments which would far outweigh the benefits accruing from the acts[43].

[41] Ben Johnson, 'Do Criminal Laws Deter Crime? Deterrence Theory in Criminal Justice Policy: A Primer' (2019) MN House Research Department 5.
[42] Ibid.
[43] Ibid.

Straub in his study posits that the deterrence theory can be extended to cybercrime which is similarly engaged in by offenders due to the perceived benefits it may attract[44]. According to the theory, offenders would be deterred from committing cybercrime based on the certainty and severity of available punishment.

The theory is therefore relevant to the researcher's study which assesses the impact of the cybersecurity legal framework in deterring commission of cybercrimes in Kenya. The theory however presupposes that punishment is the only effective deterrent against commission of crimes which is rather limiting. As a result, to ensure a holistic theoretical approach for the study, the researcher will also utilize the situational crime prevention theory which is more expansive.

1.6.2 Situational Crime Prevention Theory (SCP)

As the word "prevention" connotes SCP is a concept aimed at stopping crimes before they occur. It achieves this by making it more difficult to commit the crime as well as by minimizing the rewards that may be realised.

Ron Clarke envisioned the SCP approach as involving specified crimes whose immediate environment of commission could be manipulated with a view to increasing risks of committing the crime while reducing opportunities to commit the said crimes[45].

[44] Nicole Beebe and Srinivasan Rao, 'Using situational crime prevention theory to explain the effectiveness of information systems security' (The 2005 SoftWars Conference, Las Vegas, November 2005) 14.
[45] New Zealand Government, 'Situational Crime Prevention: Evidence Brief' (*New Zealand Government*, April 2017) <https://www.justice.govt.nz/assets/Documents/Publications/Situational-Crime-Prevention.pdf> accessed 23 June 2021.

The SCP concept is premised on the assumption that crime occurs when a likely offender is presented with available targets and opportunities which pose high rewards and are not well guarded[46]. A classic example of such a convergence is an unmanned well stocked shop or an open car window with bags and other items in full display at the parking lot or in traffic jam.
An offender would more likely commit a crime of theft under those circumstances as opposed to trying to rob a well secured facility.

SCP therefore presupposes that where the properties of a situation for commission of a crime change, for instance absence of an available target or a well-guarded opportunity with risks outweighing benefits, such crime would not take place whether or not there is a likely offender.
Its success is evident in certain SCP interventions such as introduction of engine immobilizers to reduce car theft[47] and installation of gates at alleyways offering access thereby reducing burglaries in terraced houses[48].

Whereas SCP has often been utilized in the physical realm in relation to aspects such as physical property, it can also be extended to the cyber space which has continually become vulnerable to cybercrime following increased reliance on ICT and the internet. This can be achieved for instance through applying SCP techniques such as target hardening through putting up firewalls which

[46] Ibid.
[47] Rick Brown and Nicola Billing, 'Tackling car crime: An evaluation of sold secure' (1996) Paper 71 Crime Detection and Prevention Series, Home Office Police Research Group. See also Robert Potter and Paul Thomas, 'Engine immobilisers: how effective are they' (2001) National CARS project, Adelaide, Australia.
[48] Kate Bowers, Shane D. Johnson and Alex FG Hirschfield, 'Closing off opportunities for crime: An evaluation of alley-gating' (2004) 10 (4) European Journal on Criminal Policy and Research 285, 290.

protect a network from unauthorized access and cyber intrusions thereby significantly reducing and preventing cybercrime[49].

Aside from the use of target hardening through use of firewalls, other techniques such as[50] limiting access control by setting up strong passwords regularly; denial of benefits by encrypting data; rules setting by developing a regulatory framework to address cybercrime; conscious alertness and facilitating compliance through cybersecurity training and outlining offences can also be utilized to combat cybercrime. These techniques if utilized can contribute to enhancing effectiveness of the cybersecurity framework in addressing cybercrime.

Beebe and Rao have also utilized SCP theory to assess mechanisms for cybercrime prevention. They examined the appropriateness of extending situational crime prevention theory to address physical crime in the digital realm. Their study[51] discusses the theoretical background on effectiveness of information security systems. They propose an extension of the SCP theory to accommodate aspects of the deterrence theory. They argue that potential offenders would be deterred from committing crimes based on the certainty and severity of punishment levelled. Their study highlights the benefits of extending the situational crime prevention theory to the digital realm given its ability to fill gaps of other theoretical explanations of information systems security effectiveness.

[49] Sinchul Back and Jennifer LaPrade, 'Cyber-situational crime prevention and the breadth of cybercrimes among higher education institutions' (2020) 3 (2) International Journal of Cybersecurity Intelligence & Cybercrime 25, 36.
[50] Ibid
[51] Nicole Beebe and Srinivasan Rao (n 44).

The extension of the Situational Crime Prevention theory is essential to this study due to its expanded consideration of other strategies to prevent prevalence of cybercrime including deterrence through provision of certain and severe punishment. It also buttresses the significance of using additional interventions not limited to imposition of punishments under the cybersecurity legal framework to address cybercrime such as target hardening, awareness and limited access control. The researcher will therefore rely on both theories to evaluate the cybersecurity legal framework in Kenya and the loopholes including the weaknesses if any of the existing cybersecurity legal framework and their contribution to the prevalence of cybercrime in Kenya.

1.7 Literature Review

Increasingly, services have been integrated to the cyberspace with more reliance on the internet and ICT. This has in turn increased and sustained the cyber space as a crucial medium for access to goods and services. Whereas this shift in business models has significantly enhanced access and availability of services, it has also exposed users to cybercrimes which have gained traction globally.

This review will not only support the notion that businesses have shifted to e-services but it will also outline the legal and regulatory frameworks that safeguard users against cybercrimes. It will also highlight the challenges which continue to enable prevalence of cybercrime and in the process suggest proposals to enhance cyber security by addressing cybercrime.

1.7.1 Shifting Business Models to Incorporate Use of Information Communication Technology and the Internet

Adoption of internet and ICT for business models has been considered as a key puller for customers to service industries. Okello, Bongomin and Ntayi undertook a study which established that financial inclusion was driven more by adoption of mobile money[52]. They posit that in the new age of financial inclusion through online platforms there is a need to adequately protect digital customers from risks that may arise during transactions.

According to the scholars, a failure to properly safeguard the interest of digital customers may result in diminished consumer trust and decline in use of mobile money[53] both of which would negatively affect business as well as their customers. This study therefore highlights the automation of services in the financial industry and provides a linkage to the need for all service players to incorporate proper safeguards to protect themselves and their clients from any effects which they may be exposed to due to the shift in business models.

The banking industry in Tanzania continues to evolve from the initial nationalization of private banks through the 1967 Arusha declaration to the passing of the Banking and Financial Institutions Act of 1991. Whereas the legislation did not regulate electronic banking banks nonetheless migrated to electronic banking to catch up with the global shift.

[52] George Okello and Joseph Ntayi, 'Mobile money adoption and usage and financial inclusion: mediating effect of digital consumer protection' (2020) 22 (3) Digital Policy, Regulation and Governance Journal 14.
[53] Ibid.

Banks have in the recent past integrated ICT and the internet into their business models thereby migrating their services to online platforms. This is the case in several countries including those in the East African region such as Tanzania[54].

Several benefits including more efficiency have been attributed to the change in business model for Banks in Tanzania. Electronic banking in Tanzania has been lauded for its convenience which enables users to access their accounts and multiple services from anywhere at any time without the need for long queues. The convenience however, does not come without its own risks and disadvantages. The migration has brought to the fore issues that were previously disregarded due to their relevance such as customer protection in the automated banking sphere and allocation of emergency funds to cater for loses arising from online fraud.

In view of the new circumstances, Kato's study examined the legal challenges for electronic banking in Tanzania and the remedial measures undertaken to address them including implementation of a comprehensive policy, legal and institutional framework.

The study noted that E-cheques did not have an operating framework. Customer protection was another area which was previously not considered in the electronic context despite their relevance now with more sophisticated fraud undertaken within the e-banking sphere. Banks had also not considered the need to allocate funds to cater for losses which may be suffered due to e-banking fraud. Kato's study is therefore relevant as it sheds light on the gaps which contribute to cyber

[54] Charles Ishengoma, 'Legal framework challenges to e-banking in Tanzania' (2019) 3 (2) PSU Research Review 33.

insecurity within the banking sector and proposes legal and policy changes as well as advocacy to safeguard cybersecurity in the sector.

The shift in business models is not only limited to the banking industry. Service delivery in the telecommunications industry has similarly adopted use of ICT and the internet, if Ngare's study[55] is anything to go by. The study goes further to explore security within the cyberspace for the industry and discuss challenges associated with the shift to the cyberspace.

Ngare's study seeks to answer issues affecting the telecommunication industry in Kenya for communication companies in light of the shift to the new cyber space business model. The study interrogates issues such as the protection of personal data, copyright protection, and the impact of systematic controls on content exposure and computer use. Ngare proposes the need for cybersecurity framework in the telecommunications industry which will not only remedy the issues discussed above but also provide recourse on confidentiality of personal information, data integrity, data security and data safety[56].

1.7.2 Status of Cybercrime

Whereas several service industries have managed to navigate the challenges associated with new technology users and have successfully incorporated ICT and internet to their products, security within the cyberspace continues to elude them.

[55] Benson Muriuki, 'Factors Contributing to Cyber Security Framework In Kenya: A Case Study of Kenyan Telecommunications Companies' (2018) 6 (3) Global Scientific Journals 156.
[56] Ibid.

Chitechi, Mbuguah, and Omieno conducted studies to discover the key influencers of security breaches in Kenyan county governments.[57] Their study revealed that gaps in critical cyber security infrastructure made County Governments susceptible to cyber-attacks which had increased by a whopping 108% nationally[58].

The study outlined other challenges such as the lack of proper investigative and prosecution mechanisms for cyber related offences which have contributed to insecurity within the cyber space. It also highlighted the complexity of cyber offences which mutate with advancements in technology thus requiring expertise to not only prevent them but to also investigate and properly establish a case against the perpetrators.

To address these challenges, they proposed policy formulation and awareness creation on cybersecurity attacks for end users and ICT experts as well as management. They also recommended implementation of cyber related laws where they exist and formulation of others where they fall short. Further, they recommended improvement of technologies used in prosecuting cyber offences to adapt to the fast-changing technological space[59].

Prevalence of cybercrime is another indicator of a failure to achieve cyber security. To address this, Olayinka and Babajide[60] undertook a study to interrogate the difficulties experienced in counteracting cybercrime in Nigeria. They established that the yahoo boys who were the main

[57] Kadima Chitechi, Samuel Mungai Mbugua and Kelvin Omieno, 'Facilitating factors for cybersecurity vulnerabilities in Kenyan county governments' (2018) 2 (1) Asian Journal of Research in Computer Science 1, 3.
[58] Ibid.
[59] Ibid.
[60] Olayinka Akanle and Babajide Richard Shadare, 'Why has it been so difficult to Counteract Cyber Crime in Nigeria? Evidence from an Ethnographic Study' (2020) 14 (1) International Journal of Cyber Criminology 29, 31.

perpetrators of cybercrime received insider support from the victims of their cyber-attacks and institutions mandated to prosecute the offences. The accomplices included bank officials, police officers and persons of influence such as celebrities and religious leaders as well as families. According to the scholars, the failure to achieve cyber security was further compounded by laxity to implement cybercrime law in Nigeria under the guise of non-supportive structures.

Adu and Adjei sought to determine civic awareness on cyber security amongst Ghanaian corporations. According to their findings, most internet consumers take cognisance of the attaching security risks but are unable to identify actual dangers.[61] Furthermore, they discovered that a substantial percentage of cybercrime goes undetected due to a lack of awareness. Their study goes ahead to highlight the need to conceptualise and implement training programmes on security awareness to address cyber insecurity.

Maria, Basic and Ioannis in their study[62] also sought to interrogate the extent to which African countries are responsive of cyber security concerns. They utilized a series of focus group discussions carried out in six African countries to assess their cybersecurity posture. The focus group findings captured in the form of recordings were transcribed and the qualitative data for each country analysed thematically. The study brought to the fore the need for best practice approaches for developing national awareness campaigns on cybersecurity and used these as a framework to analyse qualitative data from the focus groups.

[61] Kofi Koranteng and Emmanuel Adjei, 'The phenomenon of data loss and cyber security issues in Ghana' (2018) 20 (2) Foresight Journal 150, 151.
[62] Maria Bada, Basie Von Solms and Ioannis Agrafiotis, 'Reviewing National Cybersecurity Awareness for Users and Executives in Africa' (2019) 12 (1) International Journal on Advances in Security 108.

Their study also analysed the current state of implementation of cybersecurity awareness campaigns nationally for users and executives. It established that the sampled countries did not possess a national programme for raising awareness. This was attributed to extremely low ICT literacy levels which hindered design of cybersecurity campaigns and the underrating of the cyber insecurity challenge by executive members in organisations. The limitation of the study was however due to its sole focus on cybersecurity awareness without addressing cybersecurity laws, a conceptual gap that the current paper seeks to fill.

The European Union outlines emerging trends on cybersecurity challenges, cyber threats and attack vectors in its emerging trends 2019 report[63]. The agency outlines the rapidly evolving nature of the cyberspace landscape justifying a need for continuous capacity building on cybersecurity. The researcher's study is therefore relevant to bridge the gap on trends in Kenya which cannot be generalized from this study due to its focus on Europe.

Kwasi, Nabeel, Aminata and Martin conducted a study to highlight the current status of cybersecurity in six representative countries in East and West Africa (Nigeria, Ghana, Kenya, Rwanda, Tanzania and Uganda) with laws against cybercrime[64]. They discuss topics aligned to safeguarding cybersecurity including; internet penetration and cybercrime, misaligned incentives, successful prosecutions and the effects of legislative frameworks on cybercrime.

[63] ENISA-European Union Agency for Cybersecurity, 'Emerging Trends from January 2019 to April 2020 Enisa Threat Landscape' (*Enisa*, June 2020) <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-list-of-top-15-threats/at_download/fullReport> accessed 14 January 2021.

[64] Kwasi Adomako, Nabeel Mohamed, Aminata Garba and Martin Saint, 'Assessing cybersecurity policy effectiveness in africa via a cybersecurity liability index' (2018) Department of Electrical and Computer Engineering Carnegie Mellon University, Kigali, Rwanda 1.

The main arguments advanced in their study include the perceived focus on increasing and providing access rather than protecting the existing ICT infrastructure. They posit that the participating countries in the study suffer from some of the highest rates of cybercrime and share commonalities in the security shortcomings.

It is a key finding of the study that 97.7% of organisations fail to report any cybercrime attacks to the police. Further, it has been established in the study that in the absence of successful prosecutions there's little deterrence of perceived liability thus contributing to cyber insecurity. This study is especially relevant due to its highlighting of the correlational relationship between internet penetration and prevalence of crimes conducted through the cyberspace.

A needs assessment of cybercrime and digital evidence was conducted by Schreuders and Cockroft[65] in United Kingdom specifically, in England and Wales. The study adopted focus group discussions and directly interviewed key informants using semi-structured questionnaires. Resultant data from transcription was uploaded into NVivo for analysis.

The study findings indicated that cyber-investigation lifecycle was highly supported by cybercrime laws and policies in United Kingdom. It also highlighted instances of human rights violations in cyber-investigation lifecycles. It recommended continuous revision and improvement of the cybercrime laws in UK. The focus on UK was however limiting contextually hence the need for the study the researcher seeks to undertake to address that gap.

[65] Schreuder Cliffe and Mohammad Shan et al, 'Needs assessment of cybercrime and digital evidence in a UK police force' (2018) CARI Project, The Cybercrime and Security Innovation (CSI) Centre Leeds Beckett University 5.

Script analysis was used in a study by Leppanen, Toiviainen, and Kankaanranta to simulate a low skill level SQL injection as a type of website hacking.[66] The study sought to address identification of persons who facilitate crime as well as the stakeholders that participate in the prevention of cybercrime up to their investigation. The study reviewed data that included a real-life criminal case. They identified that it was both possible and beneficial to detect domestic perpetrators with low skill among the mass of website hacks reliant on collaboration with authorities, businesses, and organizations to put a stop to the criminals' career.

Their study recommends adoption of situation-based approaches alongside cybercrime legislation. The study's sole focus on hacking as a form of cybercrime however limits its relevance and presents a gap which the paper seeks to fill.

1.7.3 Challenges in Policing Cybercrime

A study conducted by Naci A, Bülent S and Bürke B[67] interrogated the efficacy of UK's regime in addressing cybercrime. Their analysis of other empirical studies and their research findings established that some of the challenges to policing cybercrime were; police officers having limited knowledge and expertise in responding to cybercrime incidents hence requiring expert agencies to conduct investigations. The fast evolving nature of cybercrime and lack of coordination between responsible departments in combatting cybercrime were also identified as challenges.

[66] Anna Leppänen, , Tero Toiviainen and Terhi Kankaanranta, 'From a Vulnerability Search to a Criminal Case: Script Analysis of an SQL Injection Attack' (2020) 14 (1) International Journal of Cyber Criminology 63, 65.
[67] Naci AKDEMİR, Bülent SUNGUR,and Bürke BAŞARANEL, 'Examining the Challenges of Policing Economic Cybercrime in the UK' (2020) *Güvenlik Bilimleri Dergisi* 113, 114.

The study also established that a failure to identify the perpetrator due to the nature of cybercrime being perpetuated over the cyberspace thus the perpetrator is anonymous and lack of cooperation by other States where the crime was perpetuated over territorial boundaries of the subject State contributed to the challenges affecting policing of cybercrime. A failure to preserve evidence, under prosecution due to limited capacity by investigating agencies to investigate and prosecute multiple crimes at once as well as lack of awareness on being a victim of cybercrime leading to under reporting were also highlighted as challenges in policing cybercrime. The study therefore offers a baseline for assessing the efficacy of the cybersecurity legal framework in addressing cybercrime in view of the challenges that present themselves.

1.7.4 Efficacy of Legal Frameworks in Addressing Cybercrime

Younies and Al-Tawil[68] explore the extent of protections available to businesses and citizens within the United Arab Emirates (U.A.E) under their laws dealing with cybercrime. They used the doctrinal approach to review existing laws and policies. The study established that U.A.E's cybersecurity strategy was comprehensive and was so far successful in safeguarding citizens and businesses from the unfavourable effects of cybercrime. This achievement was attributed to the passing of extensive laws and regulations with strict penalties including stiff fines and longer jail terms. The study was only focused on the U.A.E therefore it could not be generalized for Kenya hence the need for this study.

[68] Hassan Younies and Tareq Na, 'Effect of cybercrime laws on protecting citizens and businesses in the United Arab Emirates (UAE)' (2020) 27 (4) Journal of Financial Crime 1089, 1092.

Mugarura and Ssali analyse cybercrime laws and propose best practices to address regulatory weaknesses[69]. The qualitative research highlighted that inherent weaknesses at State level contribute to high incidences of cybercrimes and money laundering. They observed that regulatory weaknesses are linked to deficient infrastructure and lack of capacity of enforcement institutions. The study is therefore evidence of the need for capacity building for enforcement institutions and enhanced infrastructure to supplement legislative efforts addressing cybercrime. It is however limiting due to its focus on Uganda therefore it cannot be generalized to Kenya.

Litwaji[70] assessed the phenomenal adequacy and efficiency of cybercrime laws in Kenya. The study adopted a qualitative approach based on the relevant literature as primary and secondary data with a focus on the Computer and Cybercrime Bill of 2016. The study established that the Bill addressed issues on technology including a comprehensive range of offences such as unauthorized access, access with intention of committing other offences, child pornography as well as other computer-related crimes.

The study recommended that the drafters of the laws should from time to time monitor the progress and try to fill the lacuna in law. However, the focus on Computer and Cybercrime Bill of 2016 has been overtaken by events as it was subsequently modified to Computer Misuse and Cybercrime Bill of 2018 which was enacted as an Act of Parliament in 2018.The study will therefore focus on the present legislation and its effectiveness in that regard.

[69] Norman Mugarura and Emma Ssali, 'Intricacies of anti-money laundering and cyber-crimes regulation in a fluid global system' (2020) 24 (1) Journal of Money Laundering Control 10, 12.
[70] Clinton Mwale, 'The Phenomenal Adequacy and Efficiency of Cyber Crime Laws in Kenya' (Bachelor of Laws Dissertation, Moi University, 2017) 6.

A study by Orji examines the Cybercrimes (Prohibition and Protection) Act, 2015 to assess the extent of protections for banking and finance consumers in Nigeria[71]. It was established in the study that the existing legal regime was inadequate due to insufficient obligations requiring finance institutions including banks to protect customers' personal information from unauthorized access. This study highlights the increased reliance in electronic systems and gaps in legislation with regard to protection of consumer rights. It is however limited due to its focus on Nigeria which cannot be generalized for Kenya, a limitation the researchers' paper will address.

Whereas the review is significant in highlighting factors that have contributed to the framing of the hypothesis, it fails to adequately address the question of Kenya on all parameters which the researchers study intends to focus on. The limitation of scope therefore necessitates further research which this study intends to fulfil.

1.8 Research Methodology

Doctrinal legal research is an interrogation of existing legal doctrines as captured in law, this includes both statutory law as captured in statute as well as law as analysed in case law[72]. It also extends to a historical interrogation of previous laws or regulations and how they have influenced adoption and drafting of the existing laws in the present. It therefore follows, that this study will consider legislation which informed drafting of the existing laws which regulate the cybersecurity framework on cybercrime from a historical perspective as well as analyse the existing law as it is currently framed.

[71] Uchenna Jerome, 'Protecting Consumers from Cybercrime in the Banking and Financial Sector: An Analysis of the Legal Response in Nigeria' (2019) 24 (1) Tilburg Law Review.
[72] Khushal Vibhute and Filipos Aynalem, *Legal research methods: Teaching material* (The Justice and Legal System Research Institute, 2009) 23.

The use of doctrinal legal research will enable the researcher to test the efficiency or technical appropriateness of the legal provisions addressing cybercrime within the cybersecurity legal framework. The examination of laws and case law will therefore provide a baseline on which the researcher can assess the efficacy of the cybersecurity legal framework in addressing cybercrime in Kenya.

To analyse the existing body of literature sourced from primary and secondary sources, the researcher will use doctrinal legal research. The primary sources will include the Constitution of Kenya, 2010, Conventions, Statute, Policy documents and subsidiary legislation while secondary sources will consist of books, journals, institutional reports, opinion editorials and web-articles.

The study shall utilize doctrinal research methodology owing to the secretive nature of handling cybersecurity matters. This is discernible from the limited disclosure by victims of cybercrime including Government Ministries, Banks and Telecommunication entities on their exposure to cybercrime. It also points to the negative reception attempts to obtain primary data would face when the said entities are engaged during field research.

Additionally, disclosure of system vulnerabilities and instances of falling victim to cybercrimes would work adversely for the entities and expose them to liability claims and further attacks by cyber offenders. In view of the foregoing, the study also utilizes primary and secondary sources of data.

1.9 Delimitations

The study will face the limitation of minimal literature due to the sensitivity of cybersecurity and the overly secretive nature of dealing with system vulnerabilities and attacks to institutional cybersecurity. Further, victims of cybercrime are unwilling to share data on the cyber intrusions and attacks they have faced or have been exposed to as evidenced by limited documentation and reporting on cybercrime.

This may be attributed to the fear of liabilities which may arise following acknowledgement by any of the sector players to being victims of cybercrime. The liabilities may range from withdrawal of clients due to lowered customer confidence as well as legal suits to recover damages for losses linked to cybercrime which the said institutions ought to have safeguarded their clients against.

1.10 Chapter Breakdown

Chapter 1 – Introduction

This Chapter will provide a background of the study, introduce it and outline the problem as well as justify the study. The hypotheses, research objectives, research questions and the literature review will also be discussed in this chapter. The chapter will also identify the research methodology to be relied on for the study and the limitations thereto. Further this chapter will also outline the theoretical framework the study will rely on.

Chapter 2 – Cybercrime in Kenya

This chapter will highlight the status of cybercrime in Kenya and discuss the existing cyber security legal framework regulating cybercrime in Kenya.

Chapter 3 – Effectiveness of the Cybersecurity Legal Framework in Addressing Cybercrime in Kenya

This chapter will interrogate the effectiveness of the cybersecurity legal framework in addressing cybercrime in Kenya.

Chapter 4 - Conclusion and Recommendations

This chapter will discuss the study findings while considering their impact on the hypotheses. It will also propose recommendations and conclude the study.

CHAPTER TWO: CYBERCRIME IN KENYA

2.0 Introduction

The preceding chapter highlighted the impact technology has in improving service delivery and overall productivity in diverse sectors. It is evident that the government, businesses and members of the public have all benefited from the innovation that use of the internet and ICT has achieved in sectors ranging from health, finance, telecommunications, education and access to formal justice systems. The previous discussion also delved into the correlation between internet presence and permeation of cybercrime. Whereas the highs achieved by the shift of activity to the cyberspace are tremendous, it has also enabled criminals to navigate the cyberspace and commit cybercrimes.

This chapter will discuss the cybercrime in Kenya particularly; the different types of cybercrimes experienced and interventions put in place to counter them, both legislative and institutional. The outline will shape the discussion in the next chapter on analysing the utility of the existing regime in deterring and prosecuting cybercrime and challenges faced in that endeavour.

2.1 Cybercrime Landscape in Kenya

Common terms which have in some instances been used interchangeably when referring to unauthorised or unlawful acts committed on the cyberspace are cybercrime and cyber-attack. Cybercrime is a term loosely used to refer to criminal offences which are perpetuated over the cyberspace using the internet, information communication and technology and computing devices. Whereas cyber-attack is the purposeful exploration of computer systems and technology dependent

networks, that is done without authorisation or contrary to the law[73]. Some cyber attacks therefore constitute actions which result in commission of a cybercrime as prescribed in law.

Cybercrimes can be categorised in two broad categories[74], these are computer focused cybercrimes and computer assisted cybercrimes. Computer focused cybercrimes are those which are committed through computer systems and other enabled technologies and rely on both for their successful execution. Computer assisted cybercrimes on the other hand are those which are committed through computer systems and enabled technologies but rely on the vulnerabilities and potential errors of human beings for successful execution. Later, in this chapter, the different types of cybercrimes including phishing, unlawful interception of messages, publication of pornography, unauthorised disclosure of passwords, computer fraud, cyber harassment, cybersquatting, cyber terrorism and false publication as enumerated in the existing cybersecurity legal framework in Kenya will be discussed.

Individuals, companies and institutions including Government agencies have increasingly become targets of cybercrime which is often motivated by economic gain but may also be used to tarnish reputations. The previous chapter established that internet presence has rapidly increased across the globe with more services being integrated for utilization within the cyberspace in diverse sectors. Various sectors now offer e-Government services spanning from education, administration and civil registration.

[73] Valdemar Sousa, 'A Review on Cyber Attacks and Its Preventive Measures' (The Digital Privacy and Security Conference, 2019, Lusofona University of Porto, Portugal) 4.
[74] Sarah Gordon and Richard Ford, 'On the definition and classification of cybercrime' (2006) 2 (1) Journal in Computer Virology 13, 15.

The Government has for instance adopted use of the National Education Management Information System (NEMIS) platform in the education sector.[75] It has also utilised iTax[76], Integrated Financial Management Information System (IFMIS)[77], TIIMs and e-Citizen for tax, procurement and transport administration and civil registration purposes respectively.

Businesses have similarly shifted to use of ICT and the internet especially the financial services sector where banks, telecommunication and lending companies have moved to the digital space through innovations such as mobile banking for most commercial banks and mobile lending applications such as Tala[78] and Mshwari[79].

The shift has further been accelerated in the wake of Covid-19 which necessitated having a new way of conducting businesses, offering services and communicating. Limited physical interactions in line with mitigation measures meant that families had to shift to video calls and video conference meetings to stay in touch. The Government similarly transitioned to conducting virtual meetings and workshops due to limitations on in person gatherings. Learning institutions and other institutions such as the judiciary also adapted to the technological trends and began offering virtual classes and virtual court sessions respectively to ensure continuity of service delivery.

[75] This is a web based data management system used to collect data from different education institutions to enhance decision making and planning in the education sector. It collects data on schools and learner information and enables education agencies to share collected information online.
[76] This is an online service area administered by the Kenya Revenue Authority (KRA) where KRA pin holders can access services remotely.
[77] It is a web based integrated system which allows users both from National and County Government to plan their budgets, procure, reconcile revenue and payments and report on the financial situation.
[78] This is a global technology company which offers accessible digital financial services such as loans at the touch of a button.
[79] This is an online savings and loan service accessible to Mobile money customers operating M-Pesa accounts.

In spite of the benefits of using the internet and information communication technologies, it has also attracted disadvantages such as increased viability for victims of cybercrimes. This is evident from the statistics on cyber threats and intrusions which have occurred within the last financial year, 2020/2021 which was indicative of prevalence of cybercrimes.

According to the National KE-CIRT/CC a total of 158,405,656 cyber threats were detected within the financial year 2020/2021 out of which 38,776,699 were those recorded between April and June 2021[80]. According to the National KE-CIRT/CC cyber threats within the last quarter of the financial year were a notable increase of 37.27% from those detected between January and March 2021 which was largely attributed to increased utilization of internet and ICTs[81]. It is further reported that in the same April to June 2021 period, cyber threats culminated in investigations of a total of 529 cases which included 57.1% impersonation cases and 18.3% online fraud cases[82].

The increased shift to remote working as a mitigation measure to minimize the spread of Covid-19 was also a catalyst to increase in commission of cybercrimes within the last financial year. More users increasingly used the cyberspace to offer services and access them as they conducted their day-to-day work activities while working remotely. This also resulted in an upsurge in utilization of video conferencing applications such as Zoom, Google Teams and Google Meet which permitted virtual face to face engagement for meetings and trainings.

[80] National KE-CIRT/CC, Cybersecurity Report (April-June 2021).
[81] Ibid.
[82] Ibid.

Types of cybercrimes:

1. Phishing

Phishing is carried out by cyber-criminals with the intention of obtaining confidential information from a victim who discloses the said information assuming the requester is a trust worthy source. Often the criminals send an email request to the victim asking or prompting for the confidential information to be given by the victim.

This can be achieved through requiring something as mundane as clicking an attachment or updating a password through a request directed to the victim. The confidential information obtained by the cyber-criminal thereafter enables them to impersonate the victim and commit further fraudulent activity such as accessing credit cards or bank accounts to defraud the victims. The cyber criminals also took advantage of the convenience that lured more users to rely on e-commerce and used the cyber-attacks and intrusions to compromise the systems and gain unauthorized access to personal as well as corporate resources[83].

Cyber criminals also adapted and used the applications to undertake phishing attacks. Some would impersonate and schedule online meetings with malicious links which they used to plant malware through email alerts and unlawfully obtain data and login credentials from unsuspecting users[84].

[83] Ibid.
[84] Ibid.

The National KE-CIRT/CC in their report observed that E-commerce platforms were also victims of phishing attacks, which increased between April to June 2021 using search engine phishing emails[85] and email phishing voice.

2. Web application attacks

This are attacks which take advantage of vulnerabilities in web applications to redirect information of users to other sites or unknown intruders without their consent or authority who subsequently use the data for illegal activity. Recent statistics indicate that web application attacks have significantly increased due to utilization of cloud-based infrastructure, especially for online learning and crowd working where students and employees could access resources from any location. Cybercriminals have similarly adapted and launched increased web application attacks against the servers in an attempt to obtain unauthorized access and steal credentials of the authentic users[86].

3. Distributed Denial of Service (DDOS) Attacks

This attack is perpetuated through causing an online service to become unavailable or bombarding a site with a lot of traffic from diverse sources. The cybercriminal can subsequently access the compromised system when the network is down or to avail the data to other third parties without consent.

[85] A phishing email is an email which is sent to a potential victim from a cyber-criminal with the intent of stealing confidential information which the victim ought to have kept private. This is often done through falsely using trustworthy sources which lure the victim to open the email which thereafter asks the victim to input private information to access or gain something.
[86] National KE-CIRT/CC (n 83).

4. Identity theft

This cybercrime is perpetuated when an intruder gains unauthorised access to a user's personal information and utilises the access to commit crimes using the user's identity. This can range from using a user's account to claim for benefits, participate in criminal activity or even gain information.

5. Cybersquatting

This occurs when a person intentionally uses a name or identity belonging or registered to another without their authority.

6. Cyber harassment

It is akin to harassment perpetuated in the physical realm which involves a person intentionally communicating with another in the cyberspace in a manner that causes the recipient to be apprehensive of fear of violence, damage or loss of property.

The perpetuation of the aforementioned cybercrimes raises privacy and financial concerns. On one hand, victims are exposed once their confidential information is obtained by criminals who can use it to black mail them, commit criminal acts while impersonating them or even lock them out from accessing their accounts or platforms to their own detriment. The victims are not only individuals but also include Government Departments and Agencies, Banks, Telecommunication companies and Savings and Credit Cooperative Societies (SACCOs|) as evidenced by the

increased cases being examined by the Directorate of Criminal Investigations (DCI) Digital Forensics Laboratory[87].

Financially, once cyber criminals gain access or control over an individuals or corporations account they can easily transfer funds or publish information benefitting their competitors thus negatively affecting their business edge. In the last year alone, the President highlighted cyber security as an increasing challenge in Kenya which also threatens national security[88]. The report highlighted the cost of cybercrime to the Kenyan economy being approximately Kenya Shillings Twenty-Nine Decimal Five Billion.

These cybercrimes and a host of new emerging cybercrimes has gained traction in Kenya due to increased utilization of the internet and ICT and they continue to be perpetuated despite the existence of a cybersecurity legal framework. A consideration of the interventions initiated to counter cybercrime is therefore important for this study. These includes having specialised expertise for forensics to detect cybercrimes as well as collect admissible and relevant evidence of the commission of cybercrimes. Enhanced awareness creation to promote cyber hygiene thereby ensuring that users do not access insecure websites or open suspicious emails and links[89].

The legal framework also ought to have a mechanism for addressing emerging technologies which continue to be developed such as deepfake which enables a cybercriminal to generate almost identical information to create an illusion that the information is from a trusted source.[90] The legal

[87] Government Printer, Annual Report to Parliament on the State of National Security (Nairobi, March 2020).
[88] Ibid.
[89] The National KE-CIRT/CC, Cybersecurity Report (January - March 2021).
[90] Ibid.

framework should therefore create a framework for ensuring the public and specialised officers are aware of how to detect emerging technologies that perpetuate cybercrime with a view to investigating and prosecuting them.

The interrogation will enable the researcher to highlight the existing measures in the cybersecurity institutional and legislative framework that address cybercrime in Kenya thereby informing the analysis on its effectiveness in Chapter 3 of this study.

2.2 Countermeasures to Address Cybercrime in Kenya

2.2.1 Legislative and Institutional Framework Addressing Cybercrime in Kenya

A. REGIONAL LEGAL FRAMEWORK

The researcher will analyse the existing legal provisions regulating cybercrime and cybersecurity regionally. However, Kenya is not a signatory to either of the Regional Conventions which shall be considered in this chapter. The two conventions are however relevant to the study because they offer the first shared understanding on how to classify and address cybercrime. The focus on the regional framework addressing cybercrime is therefore utilised as a baseline for framing of cybercrime offences, measures to support the fight against cybercrime and other provisions as captured in the laws regulating the sector in Kenya.

Convention on Cybercrime (Budapest Convention)

The Convention on Cybercrime (CoC)[91] provides guidance on drafting cybercrime legislation for State parties. It prescribes substantive criminal law offences. It calls on its state parties to prescribe

[91] Council of Europe Convention on Cybercrime, CETS No. 185.

offences addressing both data protection and cybercrime. The Convention addresses issues relating to upholding the integrity of personal data and the computer systems. It also prescribes several offences which have greatly been reflected under the Kenya's regime, namely, offences related to unauthorized access and interception, and the interference of data and computer systems.[92]

It also outlines procedural law for purposes of securing evidence and conducting investigations which aid in collection and preservation of evidence as well as search and seizure. In addition, it requires State parties to adopt procedural measures for undertaking investigation and prosecution[93] to aid in collection of evidence, preservation of data as well as search and seizure. It further prescribes measures to safeguard international cooperation and mutual assistance[94] in addressing cybercrimes noting the fluid nature of cybercrimes which are not restricted by physical territorial boundaries of States.

Convention has also been instrumental in capacity building initiatives and it has assisted several countries enhance their capacities on undertaking investigations and prosecutions as well as adjudication of cybercrimes and crimes relying on electronic evidence.

Whereas it was formulated to geographically cover States which are within Europe, it has been adopted by other countries from other regions such as Africa and the Americas[95]. Ghana for instance is a State party to the convention yet it falls within the African region. Further to that,

[92] Ibid, article 2 - 12.
[93] Ibid, article 14(1).
[94] Ibid, article 23 and 25.
[95] Council of Europe, 'Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY' (*Council of Europe*, June 2021) <https://www.coe.int/en/web/cybercrime/parties-observers>accessed 22 September 2022.

several Non-State parties have reformed their legislations to conform to the provisions captured under the Convention.

According to a survey concluded in February 2020, it is estimated that an approximate 92% of States worldwide, the equivalent of 177 States are actively reforming their legislation or have completed the process of reform with a view to mirroring provisions of the CoC.[96] Out of that percentage, it is estimated that other States[97] which are not parties to the Convention have similarly drawn inspiration from it while reforming their legislation.

The survey also reports that an approximate 106 States domesticated provisions on criminal offences prescribed under the CoC. A further 82 States have also created specific procedural powers to aid in investigation of cybercrime as well as collection of electronic evidence. Mauritius[98] and Portugal[99] are examples of States which have enacted laws addressing cybercrime that prescribe criminal offences and provide for procedural rules and international cooperation.

Other countries have also reported notable progress in their fight against cybercrime following accession to the CoC. Costa Rica for example, was able to dismantle two cybercrime syndicates after they acceded to the Convention in January 2018 and established an Anti-Cybercrime Unit which cooperates with their judicial police in investigations of cybercrime. Japan on the other hand adopted provisions addressing search, extraction of evidence and seizure which have been

[96] Council of Europe, 'The Budapest Convention on Cybercrime: Benefits and Impact in Practice' (*Council of Europe*, July 2020) <https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac>accessed 22 September 2022.
[97] An approximate 153 States which are members of the United Nations have used the Convention on Cybercrime as a guideline to reform their laws addressing cybercrimes.
[98] The Computer Misuse and Cybercrime Act, 2003.
[99] The Law on Cybercrime, 2009.

instrumental in securing evidence for prosecution of defendants operating electromagnetic records which give unauthorized commands.

The Convention is significant for its provision of an international regime for cooperation in redressing cybercrime and safeguarding of electronic evidence. Its provisions have been lauded for creating a platform for poorer State parties to benefit from international cooperation without the need to accede or ratify separate bilateral agreements. This is especially significant due to the often-transnational nature of cybercrime where more than one country is involved at the investigation or prosecution stage and would require assistance from another State. It also enables the respective State parties to safeguard electronic evidence relating to the cybercrime which can be preserved to protect its credibility and admissibility during prosecution[100].

Members States to the Convention also have the benefit of gaining membership to the Cybercrime Convention Committee which offers a platform for information and experience sharing. The platform also offers an avenue to track implementation of the Convention and generation of ideas to better tackle cybercrime.

Whereas Kenya has not ratified the CoC, its proposals have largely been incorporated in Statute laws enacted in Kenya to address cybercrimes as shall be discussed later in this chapter[101]. The adoption and domestication of its provisions is evident in the following statutes; KICA; Mutual

[100] France made a preservation request for data relating to investigations on cybercrimes such as conspiracy and electronic fraud which were being used to disable antivirus programs.
[101] The Law on Cybercrime, 2009.

Legal Assistance Act, 2011; CMCA, and DPA[102] which shall be discussed later in this Chapter. This study, therefore considered it for purposes of offering a basis which persuaded the drafting of provisions captured in Kenyan Acts of Parliament discussed later in this chapter.

African Union Convention on Cybersecurity and Personal Data Protection (AUCCPDP)

The Convention is the inaugural legal regime developed to address risks in the cyber space that are faced by African Countries. It establishes a legislative framework to handle the protection of personal data in light of the growing technology landscape.[103]

It prescribes provisions on safeguarding personal data and requires countries to implement legislative frameworks that focus on physically protecting data and punishing violation of the right to privacy[104].It also requires State Parties to create organizations tasked with overseeing data protection and ensuring compliance with the Convention, as well as ensuring that ICTs do not jeopardize public freedoms.[105]

The Convention regulates three main areas that are perceived as either unregulated or not substantially dealt within the African region. Electronic transactions, personal data protection, cyber security, and cybercrime are among the issues covered[106]. It emphasizes the need of

[102] Sylvia Ndanu and Zhang Yanqiu, 'Online content regulation policy in Kenya: potential challenges and possible solutions' (2021) 6 (2) Journal of Cyber Policy 177, 180.
[103] Preamble of the AUCCPDP.
[104] AUCCPDP, article 8(1).
[105] Ibid article 12(1) and (2)
[106] The NATO CCDCE, 'Mixed Feedback on the African Union Convention on Cyber Security and Personal Data Protection' (*CCDCE*, June 2020)<https://ccdcoe.org/incyder-articles/mixed-feedback-on-the-african-union-convention-on-cyber-security-and-personal-data-protection/ > accessed 21 November, 2021.

following national constitutions and international human rights instruments like the legislation, notably the Banjul Charter.

These is evident from prescribed provisions under the Convention as articulated under Article 24 which mandates State parties to prepare a national cyber security policy; Article 25 which prescribed the need to develop legal measures and generate legislation on cybercrime, responsibilities for national institutions, and protection of critical information infrastructure.

The Convention also mirrors the CoC through its outlining of protections for citizens on processing of personal data. Article 13 prescribes the basic principles regulating personal data. It also obligates suppliers of goods to adhere to regulations of State parties while making payments through electronic means[107] and mandates State parties to prepare a legal framework on protection of personal data[108].

However, it should be noted that Kenya is not a signatory to the Convention[109]. Critics argue that the Convention gives more power to the judicial officers to carry out surveillance[110] and access personal data[111].

The limited definitions has also been highlighted as a gap which can be pursued to unreasonably limit freedom of speech or perpetuate misinterpretation. Article 29(3) (1) (g) of the Convention is

[107]AUCCPDP, article 7(1) (a)
[108] Ibid, article 8(1)
[109] African Union, *List of Countries which have signed, ratified/acceded to the AUCCPDP* (Addis Ababa, 2014).
[110] The AUCCPDP, article 31(3) (a)
[111] Ibid.

one such example, the provision permits State parties to prescribe an offence for insults channelled through a computer system. The definition of insult is however not provided for under the Convention and is open subjective interpretation by the investigative agencies.

The Convention has also been criticized for its lack of specificity on the clear minimum thresholds for personal data protection and cyber security requirements. As a result, many governments have avoided implementing substantial regulation to safeguard against cybercrimes and violations on data protection.

Moreover, the general international law principles which permit State Parties to ratify Conventions with reservations, enables States to cherry pick on provisions they would deem binding thereby weakening effectiveness of the Convention.

In addition, the Convention prescribes exceptions in its provisions thereby permitting States to opt to tie their actions to public interest[112] thereby absolving themselves from restrictions under the Convention. The failure to prescribe reasonable parameters to be considered prior to taking actions in public interest creates a loophole which would be prone to abuse by unscrupulous State parties who would label their own vested interests as "public interest".

B. NATIONAL LEGAL FRAMEWORK

Kenya Information and Communication Act, 1998 (KICA)

[112] The AUCCPDP, article 14(2).

It is the primary legislation regulating the information and communications sector which includes broadcast media, multimedia, telecommunications as well as postal services in Kenya. The Act also introduces the aspect of cybersecurity which it defines as the protection of the cyber environment by use of regulatory guidelines and policies, as well as adopting best practices from developed economies.[113]

This is in line with both the CoC and the AUCCPDP both of which advocate for adoption of compliance standards and procedural measures to negate cybercrimes. Indeed, Chapter two of the AUCCPDP outlines standards relating to statutory authorities, harmonization, democratic principles, double criminality, international collaboration and infrastructure for safeguarding critical data.

It also discusses provision of public services electronically in particular those which are controlled and funded by the government that is, e-Government services. In the previous chapter, some of the e-Government services discussed included; iTax, e Citizen and IFMIS platforms. The Government has also rolled out portals in the education sector meant to provide e-Government services; these are the NEMIS and Kenya University and Colleges Central Placement Service (KUCCPS) platforms. NEMIS enables the Education Ministry track both learners and teaching staff to ensure proper utilization of education resources. KUCCPS online platform on the other hand provides a platform for students to apply for placement to universities and colleges under government sponsorship.

[113] KICA, s 2.

Institutions established under the Act:

Communications Authority of Kenya

In accordance with the Act, Communications Authority of Kenya licences and oversees postal, information and communication services in Kenya[114]. It facilitates electronic transactions and cybersecurity by ensuring reliable electronic records[115] while promoting public confidence in their integrity and reliability[116]. It is also tasked to minimize forgery of electronic records and electronic transaction fraud in relation to cybersecurity by developing appropriate frameworks[117]. The Communications Authority of Kenya is also responsible for preparing a framework to address cybercrime offences investigation and prosecution[118].

National Kenya Computer Incident Response Team Coordination Centre (National KE-CIRT/CC)

National KE-CIRT/CC[119] is formed under the auspices of the Communication Authority of Kenya in line with its mandate to prepare a national framework to manage cybersecurity.

The National KE-CIRT/CC mirrors the Cybercrime Convention Committee which offers a platform for information and experience sharing established under the CoC. The National KE-CIRT/CC also synchronizes response on cybersecurity incidents through collaboration with different stakeholders locally, regionally and internationally. It also builds capacity on technical

[114] KICA, s 5(1).
[115] KICA, s 83C (1) (a).
[116] KICA, s 83C (1) (c).
[117] KICA, s 83C (1) (f).
[118] KICA, s 83C (1) (h).
[119] The National KE-CIRT/CC.

information regarding computer security and cybersecurity matters while detecting and preventing cyber threats and cybercrimes. Additionally, through its quarterly reports and its briefings it offers solutions on how to address cyber threats. The reports also educate and inform the public of emerging and existing potential online scams and intrusions linked to cybercrimes which cybercriminals continue to improve.

It commenced its operations in August 2017 and has been instrumental in mapping cyber security concerns as they arise in the entire Republic of Kenya. It has developed best practice guides which not only defines key terms but it also proposes mechanisms for dealing with common challenges that may arise while using the cyberspace such as online safety, unauthorized access, malware, social engineering, identity theft and awareness[120].

Following its establishment, it has to date issued several technical advisories on prevalent cyber-crimes. These include; malware[121], sim card swap[122] and online scams[123] as well as computer security incidents. Its website which operates round the clock offers a platform for individuals and institutions alike to report cyber related incidents, report security vulnerabilities and even report instances on online child abuse at the touch of a button.

[120] Communication Authority of Kenya, *General Information Security Best Practice Guide* (2020).
[121] Communication Authority of Kenya, *Advisory by the Communication Authority of Kenya (CA) on the Emotet Malware* (2018).
[122] Communication Authority of Kenya, *Alert on Disclosure of Personally Identifiable Information (PII) Leading to Sim Card Swap Fraud* (2018).
[123] Frankline, 'Kenyans warned against returning missed international calls' *The Standard* (Nairobi, 11 May 2018).

The National KE-CIRT/CC also provides support for investigation of cybercrimes through utilization of its Digital Forensics Lab and further supports prosecution of cybercrimes through partnership with police enforcement agencies.

Communications and Multimedia Appeals Tribunal

The Tribunal is tasked with the hearing and determining complaints relating to publications or behaviour of a journalist or media company.[124] It is also mandated to hear and determine complaints on anything limiting the freedom of expression of a journalist or media company as safeguarded under the Constitution of Kenya 2010. Its mandate also extends to any action or omission taken or decision made by any person in line with the Act[125]. It may also hear and determine appeals of decisions of the CA or the Media Council.[126] It specifies the rules and compliance standards that licensed information and communication service providers who collect and control data must follow.

Universal Service Advisory Council

The Council is mandated to advise the Communication Authority and offer recommendations on policy to guide the Universal Service Fund's administration and execution.[127]

Offences:

In light of the vulnerabilities associated with provision of services over the cyberspace, the Act also prescribes offences and stipulates respective punishments pertaining to telecommunication.

[124] KICA, s 102.
[125] KICA, s 102(A) (1).
[126] KICA, s 102 F (2).
[127] KICA, s 102K.

The Act's contents reflect principles noted in both the CoC and the AUCCPDP, which serve as a model for developing cybercrime law with a human rights-based approach[128].

The offences prescribed under the Act are applicable to individuals and entities working in the information communication sector. The offences can be conducted in relation to:

a) Systems and devices

The Act lists improper system usage as one of the offenses. This crime is committed when a person sends a threatening, indecent or offensive message using a licensed telecommunications system.[129] In such a case, a person would be guilty of the offense only by their conduct (actus reus), with no regard for their purpose (mens rea).

This crime can also be committed when a person sends a false message over a telecommunication system with the goal of causing irritation, discomfort, or unnecessary worry to another person. The offense requires the proof of both the conduct and the intention.

In such a case, the prosecution would be able to maintain a conviction if they could show that the conduct of sending a message while knowing it was false was done with the goal of causing irritation, discomfort, or unnecessary concern to another person. On conviction, a person found responsible is liable to pay a fine or serve imprisonment, or both.[130]

[128] Sinesipho Ralarala, 'The Impact of cybercrime on e-commerce and regulation in Kenya, South Africa and the United Kingdom' (Master of Laws Thesis, Strathmore University, 2020) 6.
[129] KICA, s 29.
[130] Ibid

The Act also provides for the offense of possessing or supplying anything for the purpose of reprogramming a mobile phone. A person is culpable if they are in custody or have under their control anything that could be used to change or interfere with the programming of a mobile phone device with the intent of using the thing unlawfully for that purpose or allowing its unlawful use for that purpose.[131]

Possession in this respect is not an offence unless that object which is held is used unlawfully to modify or interfere with how mobile phone equipment operates. The offence is therefore committed only if someone is determined to be in possession o f something with capability to interfere with functioning of a mobile phone device and has the pu rpose to utilize it illegally or enable its unlawful use.

It is also illegal to supply someone with anything that may be used to modify or tamper with the operation of mobile telephone equipment. A fundamental part of the offence is knowing or believing that a recipient of the supply will use it unlawfully or will allow it to be used in an unlawful manner to modify or interfere with how the mobile telephone equipment operates.[132].

Section 84H also makes it a crime to provide anything that may be used to alter or tamper with how mobile telephone equipment identification operates. It is an essential ingredient of the offense that the provider should know or suspect that the recipient will use or cause it to be used

[131] KICA, s 84H (1) (a) and (b).
[132] KICA, s 84H (1) (c) and (d).

unlawfully[133]. Anyone convicted for commission of the offence is liable to pay a fine or serve an imprisonment term or both.[134] The only exception is where the use and possession of the reprogramming tool is for legitimate use for either personal or other technological review pursuits[135].

b) Messages and Publications

KICA includes rogue licensed telecoms providers among the offenses (intermediaries). The Act proscribes persons involved in the operation of a licensed telecommunication system from knowingly manipulating or tampering with the contents of a message delivered over the system other than in the course of their duties. Modification, interference, interception, and disclosure are only permitted when done in the course of business. If convicted of the offence of message alteration or interference, the individual is liable to pay a fine or serve a jail term or both.[136]

It also prohibits telecommunications operators from intercepting and disclosing messages that are not in the course of their business.[137]A person convicted of interception and disclosure is liable to pay a fine or serve a jail term or both.[138]

The Act also protects telecommunications plants against interference. It makes it an offence for anyone to wilfully tamper with the telecommunication plant with a view of preventing, obstructing, or delaying message dispatch, or interfering with its operations or management. It is also an

[133] KICA, s 84H (1) (e) and (f).
[134] KICA, s 84 H (2).
[135] KICA, s 84I.
[136] KICA, s 30.
[137] KICA, s 31.
[138] Ibid.

offence if the tampering leads to unlawful interception or acquaintance with the contents of any message in a manner that prejudices the interests of the plant.[139]

A person would be found culpable for the offence if their actions are wilful and are aimed at causing obstruction, delay, prevention or interception of messages. Section 32 prescribes punishment for commission of the offence to include payment of fine, serving a jail term or both.

The Act also proscribes publication, transmission, or inducing the publication of obscene information resembling pornography in electronic form. It attracts the payment of a fine, serving a jail term or both.[140]

It also criminalizes the creation, publication, or making of electronic signatures for fraudulent purposes.[141] The intention (mens rea) underlying the publishing is critical in demonstrating the commission of the crime. A person convicted of publishing for fraudulent purposes is liable to pay a fine, serve a jail term or both.[142]

Investigations under the Act:

Investigations in relation to criminal offences are ordinarily the preserve of police officers under the auspices of the National Police service. However, the Act prescribes differently.

[139] KICA, s 32.
[140] KICA, s 84D.
[141] KICA, s 84E.
[142] Ibid.

It prescribes that investigations in relation to searches of premises are to be carried out by persons authorised by the Communication Authority in conjunction with police officers[143]. The collaboration between the Communication Authority and Police officers is significant given that the officers from the Communication Authority are more technically equipped to identify what is relevant to the offence they are investigating. As a result, the search would yield evidence which is not only admissible but relevant to the criminal action being investigated.

Search of premises is however subject to issuance of a search warrant by the Resident Magistrates courts which is permitted to issue warrants to conduct searches for premises, vehicles, vessels or aircraft with a view to testing a station or apparatus or obtain such thing or article in relation to an offence under the Act[144].

A search warrant is issued subject to proof that a notice of a demand for access of not less than seven days' has been served on the relevant person, and the same has been unreasonably denied.[145]This requirement may however work against the investigation and evidence gathering exercise since the suspected perpetrator would have notice in advance to interfere with proof of commission of the criminal offence being investigated before the investigating authorities even commence their work.

The Act permits seizure and detention of communication-related apparatus, articles or such other things found during searches where they appear to have been used in commission of the offence

[143] KICA, s 89(1).
[144] KICA, s 89.
[145] KICA, s 89(2) (b) (ii).

or could be used as evidence[146]. Property seized in relation to a search warrant may be detained until the expiry of six months after the seizure or after the conclusion of proceedings where they are initiated or at such other period as the court may order[147].

Prosecution under the Act:

Public prosecutions in respect of criminal offences are carried out by the DPP. However, the Act makes an exception for offences under the Act. The offences may be prosecuted by officers authorized in writing by the Communication Authority, especially where the DPP has donated prosecutorial powers in line with the constitution.[148]The authority conferred by dint of section 104(1) of the Act offers an opportunity for officers with specialized technical knowledge to prosecute offences under the Act as opposed to leaving it to prosecutors who only have a general grasp of the offences.

The grant of prosecutorial powers to the Communication Authority is significant, since it not only provides an avenue for timely prosecution and faster enhancement of controls, but it also addresses the question of bureaucracy which would have ordinarily required engagement of the Directorate of Criminal Investigations (DCI) and the ODPP prior to commencing prosecution.

The involvement of the Communication Authority is also significant because it offers a technical knowledge base right from the onset of investigations. As a result, digital evidence which is often technical is handled and stored in a manner that safeguards its admissibility.

[146] KICA, s 90.
[147] KICA, s 92(1).
[148] KICA, s 104(2)

Mutual Legal Assistance Act, 2011

It provides a framework for collaboration and assistance between requesting States, International entities and Kenya for criminal matters investigation, prosecution and judicial proceedings[149]. This corresponds to provisions under both the AUCCPDP and the CoC. The provisions obligate State parties to develop legal frameworks focused on safeguarding physical data and punishing privacy violations[150] and adopt procedural measures to safeguard international cooperation[151] and mutual assistance[152] in addressing cybercrimes noting the fluid nature of cybercrimes.

Cybercrimes can be perpetuated outside the territorial jurisdiction of a country with victims being within the territorial jurisdiction. The Act is therefore significant for the latitude it presents for prosecution and investigation of cybercrimes which are not restricted to physical territorial boundaries. It provides a framework for collaboration between different States which is significant for cybercrimes which can be committed by persons who are outside the territorial jurisdiction of Kenya but impact persons within the territory of Kenya.

Provisions relating to legal assistance[153] provide an avenue for ease in identification and location of cyber criminals, examination of witnesses who are out of territorial jurisdiction of the requesting State, carrying out of searches and seizures, examination of objects and sites as well as preservation of communications data. Hearsay or a statement of opinion is admissible as evidence under the Act in a proceeding where the court has jurisdiction provided the probative value can be

[149] Mutual Legal Assistance Act, 2011, section 3.
[150] AUCCPDP, article 8(1).
[151] Council of Europe Convention on Cybercrime, CETS No. 185, article 23.
[152] Ibid, article 25.
[153] Mutual Legal Assistance Act, 2011, s 6(2).

examined[154].Other States can also benefit from the provisions of legal assistance which similarly permit them to submit requests to the Central Authority[155].

In view of technological advancements, the written requests also include e-mail, facsimile and other agreed forms of electronic transmission subject to authentication[156]. Regardless of the need for reciprocity Kenya has the latitude to decline a request for legal assistance[157].

The exception is permissible if the request relates to an action which is not punishable in Kenya; and is subject to limitation of actions due to lapse of time had it been an offence against Kenyan law or such a person had been acquitted or pardoned in the requesting State. This exception also applies where the request is for an offence of political nature or it is for prejudicial prosecution or punishment on discriminatory grounds such as race, sex, religion, nationality or political opinions. Kenya may also decline a request for legal assistance where granting it would harm the Country's sovereignty, security or such other national interest as well as where it would likely jeopardize a person's safety.

Kenya is obligated to co-operate in proceedings to identify and ultimately forfeit proceeds and instruments of crime at the behest of the requesting State[158]. The co-operation includes permitting authorities of the requesting State to confiscate assets,[159] permitting confiscation of property

[154] Ibid, s 33.
[155] Ibid, s 8(1).
[156] Ibid, s 8(3).
[157] Ibid, s 11.
[158] Ibid, s 23(1).
[159] Ibid, s 24(b).

without a criminal conviction where the accused cannot be traced[160] and permitting competent Kenyan authorities to undertake such activities subject to an order of the same.[161]

Co-operation in respect of recovery, freezing, confiscation and disposal of assets may be declined if the requesting State fails to adduce enough evidence or where the worth of the asset is negligible.[162]

Institutions established under the Act:

The Mutual Legal Assistance Act, 2011 establishes a Central Authority which is tasked with coordinating legal assistance by transmitting, receiving and processing the requests[163].The legal assistance is wide ranging to include examination of witnesses, service of court pleadings, execution of searches and seizures to taking of evidence, safeguarding of communication data and conducting covert electronic surveillance.[164]

Computer Misuse and Cybercrimes Act, 2018 (CMCA)

Engagements on a legal framework to address cybercrime in Kenya were initiated through the Computer Cybercrimes Bill of 2016 which only bore fruit in 2018 when Act was enacted.

[160] Ibid, s 24(c).
[161] Ibid, s 24(d).
[162] Ibid, s 25.
[163] Ibid, s 6(1).
[164] Ibid, s 6 (2).

Enactment of the Act was criticised for its vagueness especially on the definition of prohibited conduct and its provision on prohibition of hate speech[165]. Additionally, questions were raised regarding the delimitations on authorities' powers of surveillance, and whether the powers were violating the constitutional right to privacy.

The Act was also challenged for allegedly violating constitutional rights and freedoms, whereupon the court suspended some of its sections.[166]

The LSK also subsequently joined and supported the petition. They argued that it contained questionable provisions which posed a risk to the Bill of Rights specifically on arrest and prosecution[167]. In their pleadings, the LSK highlighted the freedom of expression which they opined would be infringed on. It was their contention that in a democracy, the public enjoy freedom of expression without their expressions being termed as hate speech. They further contended that some of the sections were too vague and broad that they prejudiced the public's right to information.

Mr George Maina also reiterated the grounds advanced by LSK and BAKE.[168] He argued that the Act was passed without public participation and that the provisions on asset confiscation infringed on the right to protection of property. The petitioner's case also weighed in on the severity of the

[165] Mercy Muendo, 'Kenya's new cybercrime laws open the door to privacy violations, censorship' The Conversation (Nairobi, 29 May 2018) 11.
[166] *Bloggers Association of Kenya (Bake) v Attorney General & 5 others* [2018] eKLR.
[167] Lolyne Ongeri, 'LSK challenges the constitutionality of the Computer Misuse and Cybercrimes Act' (*Ifree*, June 2018) < https://www.ifree.co.ke/2018/06/lsk-challenges-constitutionality-of-the-computer-misuse-and-cybercrimes-act/> accessed 20 November 2021.
[168] Victoria Wangui, 'Petitioner challenges the Computer Misuse and Cybercrimes Act' (*Ifree*, May 2018)< https://www.ifree.co.ke/2018/05/petitioner-challenges-computer-misuse-and-cybercrimes-act/> accessed 20 November 2021.

penalties, arguing that the penalties hindered the public from exercising their freedom of expression.

The Act was also challenged for not having the input of the senate during the enactment process. The High Court which heard the matter subsequently declared the Computer Misuse and Cybercrimes, 2018 unconstitutional hence null and void.[169]

The judgement was subsequently appealed against before the Court of Appeal, whereupon the appellate court overturned the High Court's decision, thus reinstating the Act.[170]

Whereas KICA focused more on the regulation of the telecommunication sector and broadcast services, CMCA specifically focuses on cybercrime in Kenya and globally through mutual legal assistance.

The Act mirrors provisions of the CoC, under which state parties are required to introduce procedural measures with a view to safeguarding international cooperation[171] and mutual assistance[172] in addressing cybercrime. In the same breadth, it also incorporates provisions of the AUCCPDP which also obligates member states to establish regimes focused on physical data protection and punishment of privacy violations.[173]

[169] *Senate of the Republic of Kenya & 4 others vs. Speaker of the National Assembly & another ; Attorney General & 7 others (interested parties)* [2020]eKLR.
[170] *Speaker of the National Assembly & another v Senate & 12 others (Civil Appeal E084 of 2021)* [2021] KECA 282 (KLR) (19 November 2021).
[171] Council of Europe Convention on Cybercrime, CETS No. 185, article 23.
[172] Ibid, article 25.
[173] The AUCCPDP, article 8(1).

CMCA is the first holistic legal framework of its kind in Kenya which comprehensively addresses cybercrimes. Its scope of application is reflective of the prevailing times based on its expansive definition of a computer system[174]. It recognises that mobile devices have almost similar capabilities as laptops and computers hence are susceptible to similar intrusions leading to cybercrime offences.

The Act establishes a committee which provides advisories to the Government and coordinate activities relating to computer and cybercrimes.[175] The committee is mandated to coordinate the investigation of cyber threats and respond to cyber incidents threatening the Kenyan cyberspace whether or not the said threats or incidents originate within or outside our territorial physical boarders[176]. The committee is also charged with developing a training framework as a countermeasure to address prevention and detection of computer and cybercrimes[177].

Institutions established under the Act:

National Computer and Cybercrimes Co-ordination Committee (NCCCC)

The committee mirrors the Cybercrime Convention Committee established under the CoC. It is also a coordination organ. Its overall mandate is providing advisory and coordinating computer and cybercrime issues which happen in and outside Kenya. The committee is tasked with formulating strategies to assist in training agency personnel on how to mitigate, prevent and detect

[174] CMCA, s 2.
[175] CMCA, s 4. The National Computer and Cybercrimes Co-ordination Committee (NCCCC).
[176] CMCA, s 6(1) (f).
[177] CMCA, s 6(1) (j).

cybercrimes[178] as well as coordinating responses to threats of computer and cybercrime incidents[179].

It is also mandated to establish guidance notes and standards for cyber-security practice and performance for critical national information infrastructure[180]. It is also tasked with administering a national public key infrastructure framework[181]. Further, the committee is also required to advise the National Security Council,[182] as well as receiving and acting on reports on computer and cybercrimes.[183]

It draws its membership from representatives in the justice system such as the National Police Service[184], National Intelligence Service[185], ODPP,[186] and the Office of the Attorney General (OAG)[187] as well as representatives of security organs and Ministries, including the Ministry responsible for internal security[188] and the Kenya Defence Forces[189].

The committee is also comprised of members from; the Ministry responsible for ICT[190], the Communication Authority of Kenya[191] and the Central Bank of Kenya[192]. The composition drawn

[178] CMCA, s 6(1) (j).
[179] CMCA, s 6(1) (g).
[180] CMCA, s 6(1) (h).
[181] CMCA, s 6(1) (i).
[182] CMCA, s 6(1) (b).
[183] CMCA, s 6(1) (d).
[184] CMCA, s 5(1) (e).
[185] CMCA, s 5(1) (f).
[186]CMCA, s 5(1) (h).
[187] CMCA, s 5(1) (c).
[188] CMCA, s 5(1) (a).
[189] CMCA, s 5(1) (d).
[190] CMCA, s 5(1) (b).
[191] CMCA, s 5(1) (g).
[192] CMCA, s 5(1) (i).

from diverse sectors is indicative of those who are most affected by cybercrimes which include the Banking and Finance Sector, the Criminal Justice Sector and the Information, Communication and Technology Sector.

Whereas the committee was established by statute in 2018, it was only operationalized three years later[193] following its launch on 4th November 2021. Its inaugural focus was on prioritizing social media misuse ahead of the upcoming 2022 general elections and safeguarding online safety in view of technological advancements. Its impact is therefore yet to be seen as it is too early in the day to report on its work hence need for further research to assess its effectiveness in addressing cybercrime.

Offences under the Act:

Part III outlines the offences punishable under the Act. Similar to some of the offences highlighted under KICA, CMCA also addresses offences relating to unauthorized access, interception or disclosure, fraudulent use of electronic data as well as publication of false materials.

It further addresses the issue of pornography with a specific focus on child pornography which is reflective of the challenge being experienced with enhanced access to mobile devices and computers that children have access to in the current times. The offences under the Act have also adapted to the advancements that cybercriminals have used to undertake sophisticated attacks such as cybersquatting and phishing.

[193] Bruhan Makong, 'Kenya Unveils National Computer and Cybercrimes Co-ordination Committee to fight Cybercrime' *Capital News* (Nairobi, November 4 2021) 6.

The offences under the Act are carried out on:

a) Computer systems and Critical infrastructure

Access to a computer system without authorisation and through manipulation of security measures is an offence punishable upon conviction by a prison sentence or payment of a fine or both.[194] The element of the action being unauthorized and being used to manipulate security measures to gain access qualifies it as an offence punishable under the Act. It also prescribes an additional offence, where such commission is to aid commission of a further offence or to facilitate its commission which is punishable by payment of a fine or serving a jail term or both.[195]

This additional offence creates a leeway for punishment of other offences which are committed as a result of gaining unauthorized access through manipulation of computer systems. The offence under section 15(1) holds whether or not it is done concurrently with the offence of unauthorized access under section 14(1).

The Act also creates an offence where the target is critical infrastructure. It prescribes an offence where the unauthorized access is targeted towards obtaining access to critical data with intent to prejudice the Kenyan Republic.[196] The offence termed as cyber espionage is punishable with payment of a fine or serving a jail term or both. An additional punishment is prescribed under the Act where the offence results in physical injury of any person. In such an instance it attracts an

[194] CMCA, s 14(1).
[195] CMCA, s 15(1).
[196] CMCA, s 21 (1) (a).

imprisonment term not exceeding twenty years[197] and imprisonment for life when it causes death of a person[198].

Intentional interference with a computer system, program or data which is unauthorized is also punishable under the Act and attracts payment of a fine or serving a jail term or both.[199] The offence becomes actionable where the interference is intentional and without authority.

The Act introduces further culpability by prescribing that interference carries an additional penalty when it results in either of the following: significant financial loss, prejudices national security, death or undermines public safety and health.[200] Where the said interference causes any of the aforementioned results, the person found guilty is liable to serve a jail term, or pay fine or both.[201] The prescribed punishment holds whether or not the interference has a temporary or permanent effect[202] and whether it targets a specific computer system, data or program.[203]

It is an offence under the Act to intercept without authority and cause data to be transmitted whether directly or indirectly.[204] The offence as prescribed shall become actionable where the interception is unauthorized and is used to transmit data using a computer system over a telecommunication system regardless of whether it is direct or indirect. It attracts a jail term or payment of fine or both.

[197] CMCA, s 21 (2).
[198] CMCA, s 21 (3).
[199] CMCA, s 16(1).
[200] CMCA, s 16 (3).
[201] CMCA, s 16 (3) (d).
[202] CMCA, s 16 (5).
[203] CMCA, s 16 (4).
[204] CMCA, s 17 (1).

It carries an additional penalty where commission of the offence results in significant financial loss, death, jeopardizes national security, threatens public health or public safety.[205] A person found culpable in such circumstances is liable to serve a jail term or pay a fine or both.[206]The offence mutates to cyber espionage and carries an enhanced prison term of twenty years where it relates to a critical database data for the benefit of a foreign State against the Republic of Kenya[207] and additional penalties where it results in any physical injury[208] or death[209] of any person.

The Act prohibits persons from illegally disclosing passwords and access codes to a computerised protected program, and the same is punishable by payment of a fine, serving a jail term or both.[210] The offence is activated where the alleged offender does so without authorization for that action. The fine and prison term in the Act is enhanced in comparison to the punishment prescribed for the same offence under KICA. Persons found guilty of the offense are liable to serve a jail term or pay a fine or both.[211]

CMCA carries an enhanced penalty where the offence relates to unauthorized access, unauthorized interference or interception of a protected computer system[212]. The offence is punishable by serving a jail term, or payment of a fine or both.

[205] CMCA, s 17 (2).
[206] CMCA, s 17 (2) (d).
[207] CMCA, s 21 (1) (b).
[208] CMCA, s 21 (2).
[209] CMCA, s 21 (3).
[210] CMCA, s 19 (1).
[211] CMCA, s 19 (2).
[212] CMCA, s 20 (1).

A protected computer system in this case is one which hosts any data considered fundamental to the country's security or the fight against crime or delivery of services relating to communication infrastructure, banking and financial services[213] such as e-banking platforms, payment and settlement systems and instruments. It also extends to those relating to public utilities or transportation including e-government services such as TIIMs platform; as well as essential services on public safety like the armed forces, civil registries, and medical records among others.[214]

It also prescribes an offence for forgery committed through computer medium. Section 25(1) of the Act makes it an offence to intentionally manipulate computer data with a view to using it as authentic. It becomes forgery where the person intentionally manipulates the data and passes it off as authentic. It is punishable by payment of a fine or serving a jail term or both.

The Act prescribes an enhanced penalty if the forgery is done with a view to making some wrongful gain or economic benefit.[215] Culpability is punishable with the payment of a fine or serving a jail term or both.[216]

Fraud carried out in the physical realm is similar to fraud committed in the cyberspace as both are criminal in nature and attract a penalty. The Act prescribes the offence of computer fraud which is carried out with intent to unlawfully gain, to occasion unlawful loss or to obtain economic benefit

[213] CMCA, s 20 (2).
[214] CMCA, s 20 (2).
[215] CMCA, s 25.
[216] CMCA, s 25 (2).

to the detriment of another[217]. The elements tied to this offence are carrying out actions that are intended to result in unlawful gain, loss for the victim and economic benefit for others.

This can be done through unauthorized access to a protected computer program or data; or alteration either through additional input, deletion, generation or suppression; or copying, transfer or movement to another computer device; or using it or displaying it[218]. The offence is punishable by serving a jail term, or payment of a fine or both.[219]

Harassment undertaken within the cyberspace is also criminalized under the CMCA. It is an offence to either individually or jointly wilfully communicate with another person or such a person who is known to that person with the intention of causing them apprehension of possible violence, damage or loss of their property, negative effect to the person or grossly affect and offend them.

Cyber harassment under the Act may be committed by one or more persons jointly who intend to cause some level of apprehension due to their wilful communication with the victim. The offence upon successful conviction is punishable by payment of a fine or serving a jail term or both.[220] A victim of cyber harassment has additional relief in the form of a refraining order which they may apply for individually[221] or an intermediary may apply on their behalf.[222] In the event that such an order is violated, the perpetrator is liable to serve a jail term, or lay a fine or both.[223]

[217] CMCA, s 26 (1).
[218] CMCA, s 26 (1).
[219] CMCA, s 26 (1).
[220] CMCA, s 27 (2).
[221] CMCA, s 27 (3).
[222] CMCA, s 27 (5).
[223] CMCA, s 27 (8).

Intentional and unauthorized use of another's name, business name, trademark of other unique identifier on the internet or a computer network is a punishable offence under the Act[224]. Cybersquatting is based on the act being both intentional and unauthorized. It attracts a jail term or the payment of a fine or both.[225]

It also prescribes offences relating to identity theft or impersonation through unlawful use of a unique identification feature such as an electronic signature password. The offence is punishable by serving a jail term, or payment of a fine or both.[226]

Additionally, it also creates an offence relating to "identity theft" in relation to websites with a view to obtaining personal information through deception and using it for another unlawful purpose. The Act prescribes an offence relating to deceptive use of a website with a view to obtaining unauthorized access or illegally acquiring personal data,[227] and a person found guilty of the offence of phishing is liable to serving a jail term or payment of a fine or both.[228]

Similar to acts of terrorism undertaken within the physical realm, cyber terrorism attacks undertaken through computerized avenues are also criminal in nature and attract penalties under the Act. The offence of cyber-terrorism takes cognizance of the changing realities in the practice of terrorism which has now been integrated into the cyber realm. When one is found culpable of cyber terrorism they are liable to serving a jail term, payment of a fine or both.[229] The

[224] CMCA, s 28.
[225] CMCA, s 28.
[226] CMCA, s 29.
[227] CMCA, s 30.
[228] CMCA, s 30.
[229] CMCA, s 33 (1).

imprisonment term is however not as stringent as that in the Prevention of Terrorism Act, 2012 which prescribes an imprisonment term not exceeding thirty years.[230]

b) Messages and Publications

The technological advancements globally have resulted in the use of electronic services to transmit money from one account to another, in Kenya this is possible through e-banking which permits money transfer from mobile devices or computer systems. In light of this, and the ability of cyber criminals to take advantage of new interventions, CMCA criminalizes interception of money transfers and electronic messages. Culpability for the offence is punishable by serving a jail term or payment of a fine or both.[231]

Intentional misdirection of electronic messages is a punishable offence under the Act which is punishable by payment of a fine, serving a jail term or both.[232] Inducement to deliver electronic messages not specifically meant for them on the other hand is punishable by payment of a fine, serving a jail term or both.[233] While the offence of misdirection is based on intent of the alleged perpetrator, inducement to deliver electronic messages focuses on the recipient of the message.

Intentional withholding of another person's electronic mail, messages, electronic payments and credit or debit cards is also an offence under the Act. The action of withholding only becomes

[230] Prevention of Terrorism Act, 2012, s 4(1).
[231] CMCA, s 31.
[232] CMCA, s 32.
[233] CMCA, s 34.

criminal where it is intentional on the part of the perpetrator. Those found guilty of the offence are liable to serve a jail term or pay a fine or both.[234]

Unauthorized and illegitimate destruction of electronic mail or money transfer processes is also prohibited under the Act, and it is punishable by payment of a fine, serving a jail term or both.[235]

Whereas destruction of electronic mail or money transfer processes is not criminal, doing so without authorization and illegitimately is what results in the offence punished under the Act.

The Act recognises that it does not operate in a vacuum[236] and takes cognizance of the rights safeguarded under the Constitution of Kenya, 2010 such as when rights can be limited in line with article 24.

The Act also punishes intentional publishing of false data or misinformation under the guise of authenticity with a view to gaining some benefit. It criminalizes intentional publication of false, misleading or fictitious data or misinform to appear authentic whether financial gain is attached to it or not, and the same is punishable by serving a jail term or payment of a fine or both.[237] Where the false publication is published in broadcast, print, data or over a computer system, and it causes panic, chaos or violence among Kenyan citizens or it discredits someone's reputation, it also constitutes an offence.

[234] CMCA, s 35.
[235] CMCA, s 36.
[236] CMCA, s 22 (2).
[237] CMCA, s 22 (1).

The false publication referenced here specifies the mediums through which it is published which are not limited to computer systems but also include traditional avenues such as print and broadcast. The impact of the publication is also considered with leeway for pursuing defamation where it dishonours someone. Section 23 of the Act stipulates that the offence shall be punishable by serving a jail term or the payment of a fine or both.

It also criminalizes the publication of child pornography through a computer system or telecommunication apparatus or its possession in a computerised device.[238] The offence mirrors that of child pornography but becomes actionable where it is published or possessed using a computer system, telecommunication apparatus or computer data storage where applicable.

Persons convicted for the offence are liable to serving a jail term or payment of a fine or both. It is however a defence to possess or publish child pornography in books, pamphlets among other print media, if such publication is for public good or for education purposes.[239]

In recognition of the constitutional right to privacy and human dignity, the Act creates an offence to protect persons form ill intended transmission of intimate images. It proscribes the wrongful dissemination of another person's intimate pictures,[240] and it is punishable by serving a jail term or payment of a fine or both.[241]. For the action of distribution of obscene or intimate images of another to qualify as an offence under the act, it ought to be proved that it was wrongful.

[238]CMCA, s 24.
[239] CMCA, s 24 (2).
[240] CMCA, s 37.
[241] CMCA, s 37.

The Act also prescribes offences relating to fraudulent grant of e-instructions[242] and usage of electronic information[243] which are punishable upon conviction with fines and imprisonment terms as prescribed under the Act. Both offences mirror fraud which may be committed in the traditional physical realm; however, they now focus on electronic data and electronic instructions respectively.

Other offences and reliefs under the Act:

The Act requires an operator of a computer system to report cyber-attacks to the NCCCC of any cyber-attacks within 24 hours.[244] It further provides key information which should be submitted in support of the report[245]. Failure to make the report within 24 hours is prescribed as an offence under the Act and those convicted for the offence are liable to serve a jail term, pay a fine or both.[246]

Creation of this offence, indirectly promotes the right to access information with punitive punishments for actors who fail to comply. The requirement to notify the NCCCC of cyber-attacks, intrusions or disruptions within 24 hours[247] provides a timely knowledge base for the Committee which not only enhances its capacity to provide advice on tackling cybercrime but also enables it to propose mitigating measures.

[242] CMCA, s 39.
[243] CMCA, s 38.
[244] CMCA, s 40 (1).
[245] CMCA, s 40 (2).
[246] CMCA, s 40 (4).
[247] CMCA, s 40 (2).

The Act imposes a duty on others not to indulge cybercrime perpetrators by making criminalizing aiding and abetting cybercrimes.[248] This offence places an obligation on other individuals to be vigilant and cyber aware so as not to aid or abet the crimes, and perpetrators culpable for aiding or abetting are liable to payment of a fine, serving a jail term or both.[249]

The Act criminalizes both the actual commission of the offence as well preparatory acts in relation to commission, and those found guilty are punishable by serving a jail term, payment of a fine or both.[250]

The common adage with great power comes great responsibility has been implemented under the Act which prescribes enhanced penalties for Body corporates and persons holding high ranking position such as principal officers. The Act prescribes that body corporates who commit any offence under the Act are subjected to a different penalty of payment of a fine.

It further extends the penalty to individuals who were its principal officers or persons acting in similar capacity at the time of the commission.[251] Upon conviction for commission of the offence, the convict is required to pay a fine, or serve a jail term or both.[252] This offence shall similarly apply to members to the extent of their management actions. The only permissible defence the principal officers, persons acting in similar capacity including members (where applicable) could

[248] CMCA, s 42 (1).
[249] CMCA, s 42 (1).
[250] CMCA, s 42 (2).
[251] CMCA, s 43(1) (b).
[252] Ibid.

sustain is to prove that it was done without their consent or knowledge or in the alternative that they exercised reasonable due diligence to avert it[253].

The Act also creates a seamless linkage to other laws which prescribe offences and considers the additional impact realized from use of a computer system to commit the said offence. It imposes additional penalties for offences provided for by other written laws.[254] A person found guilty upon conviction shall be liable to the prescribed penalty in the relevant law.

The sentencing will however consider additional mitigating factors such as the impact of use of the computer system in commission of the offence[255] as well as responses to questions such as; did it enhance the impact of the offence? Was there any resultant commercial advantage or financial gain? Did it occasion responsibility breach? What was the conduct of the accused? Did it affect other persons? What was the monetary value of the loss suffered by the victim or of the profit gained by the perpetrator?[256]

Where a court convicts a party under the Act or any other Act where it is committed through a computer system, the court is vested with authority to make an order for payment of compensation for losses occasioned by the commission of the offence[257].

[253] Ibid.
[254] CMCA, s 46 (1).
[255] CMCA, s 46 (2).
[256] Ibid.
[257] CMCA, s 45 (1).

The said compensation order is recoverable as a civil debt but it does not prejudice seeking of additional relief. It can be sought through civil remedy as a claim for damages, especially where the loss suffered is higher than the monies awarded under the order for compensation.

Court may also issue an order for confiscation or forfeiture of assets, proceeds or monies obtained through proceeds arising out of cybercrimes.[258] The respective Court may further make an order of restitution of the said assets, proceeds or monies in line with PCAMLA[259].

Investigations under the Act:

The Act permits a police officer to apply for a search warrant before a court where they reasonably believe that a specified computerized device is material evidence or was acquired in commission of an offence. The warrant is utilized for search and seizure as granted and it remain active unless the court cancels it or until it has served its purpose.[260] The search warrant may also be utilized to assist a requesting State to enable them collect evidence or undertake investigations in line with mutual legal assistance provisions under the Act[261].

Investigations under the CMCA are undertaken by police officers as well as officers working under the auspices of the National Intelligence Service and the Kenya Defence Forces[262]. Designated experts and persons working with law enforcement agencies are empowered to conduct searches and seizures upon receipt of a search warrant.[263]

[258] CMCA, s 44 (1).
[259] CMCA, s 44 (2).
[260] CMCA, s 48 (3).
[261] CMCA, s 57.
[262] CMCA, s 47 (3).
[263] CMCA, s 48 (1).

The inclusion of cybersecurity experts is significant as it offers an opportunity for the search and seizure to be more targeted due to the specialized technical knowledge possessed by the cybersecurity expert.

Evidence of commission of cybercrimes can be easily erased, modified or otherwise compromised. To safeguard against this, the Act is the first legislation in Kenya to prescribe for expedited preservation of data in cases where the data might be tampered with, with a view to rendering it inaccessible.[264]

Data Protection Act, 2019 (DPA)

The Act prescribes a framework for handling personal data by outlining rights and duties of data subjects, controllers and processors. It empowers the office of the Data Commissioner to process complaints received on infringement of rights under the Act[265]. The Data Commissioner is also tasked with conducting public awareness on the measures provided for under the Act[266]. Similar to CMCA, DPA imposes a duty to cooperate on data protection within international actors to comply with obligations under international conventions and agreements[267].

The overall purpose of the AUCCPDP was to develop a credible cyberspace and respond to the gaps affecting regulation of the digital environment; thus, sharing similar tenets with the DPA.

[264] CMCA, s 51(1) (b).
[265] DPA, s 8 (1) (f).
[266] DPA, s 8 (1) (g).
[267] DPA, s 8 (1) (i).

The two legal frameworks share the mandate of establishing standards and procedures to address arising issues on cybersecurity. The duties to adopt legislation against cybercrime; which supports the DPA; and to facilitate the emergence of national regulatory authorities are prescribed under Article 25(2) of the AUCCPDP.[268]

The DPA has comprehensive provisions on how personal data ought to be processed[269] and outlines key principles that should be relied on when doing so[270]. It also prescribes mechanisms for safeguarding individuals' privacy including provisions on the establishment of regulatory mechanisms to safeguard personal data. The Act further outlines provisions giving data subjects' optimal protection and afford them remedies where their data is not processed in line with the Act. The law is applicable to processing of data subjects located within Kenya.[271]

In similar fashion, the CoC puts emphasis on safeguarding personal information and the protection of privacy as captured under the DPA. It regulates against computer data breaches and prescribes offences' relating to wrongful data interception and its usage.

Principles of Data Protection:

The Act prescribes principles and obligations relating to personal data protection. This can be used to determine intention, legitimacy and lawfulness when data is interfered with, intercepted, misdirected or otherwise tampered with and when it can constitute an offence under the other Acts previously discussed.

[268] The AUCCPDP, article 25 (2).
[269] DPA, s 3 (1) (f).
[270] DPA, s 25 (1) (c).
[271] DPA, s 4 (1) (i).

The Act requires data handlers to process personal information in a manner that is transparent, lawful[272] and upholds one's right to privacy.[273] The processing ought to be for legitimate grounds,[274] processed data ought to be relevant and the data should only be used for the stated purpose.[275] Determining intention, legitimacy and lawfulness are integral to determining the *mens rea* aspect of any actions thereby assessing whether the said action constitutes an offence or not.

Where data is processed without the owner's authorization, unlawfully and for illegitimate purposes, it would constitute an offence as shall be outlined in offences prescribed under DPA.

The Act imposes protections where the data processing relates to family or private affairs by requiring that a valid explanation is provided before such data collection takes place[276]. It further requires collected data be updated and correct[277] and that identification of data subjects is limited to necessity for the purpose for which the data was collected[278].

The Act also limits transfer of data outside Kenya unless the data subject has granted consent or there is proof that adequate data protection safeguards have been put in place[279]. The principles requiring consent of a data subject and an explanation prior to data processing are key against

[272] DPA, s 25 (b).
[273] DPA, s 25 (a).
[274] DPA, s 25 (c).
[275] DPA, s 25 (d).
[276] DPA, s 25 (e).
[277] DPA, s 25 (f).
[278] DPA, s 25 (g).
[279] DPA, s 25 (h).

protecting data subjects from cybercrimes which are committed when data is processed without consent.

Rights of a Data Subject:

A data subject refers to a distinguishable natural person to whom personal data relates.[280] They may exercise the rights on their own or through a representative where they are a minor[281], incapacitated due to mental or other disability[282] or they have duly authorized someone else[283]. Data subjects are entitled to be notified of how their personal data informed will be used,[284] they ought to have access to the data[285] and they have a right to object the processing.[286] A data subject also has a right to correct[287] and delete false or misleading data.[288]

The Act prescribes additional rights which a data subject is entitled to enjoy. Data controllers are mandated to notify a data subject before collecting personal data or their rights[289], the fact that the data is being collected[290] and the purpose[291] and other persons to whom the data will be accessible, their contacts as well as the safeguards put in place. They are also obligated to inform data subjects of security controls employed to safeguard confidentiality and integrity of the data and the law behind the collection where applicable.

[280] DPA, s 2.
[281] DPA, s 27 (a).
[282] DPA, s 27 (b).
[283] DPA, s 27 (c).
[284] DPA, s 26 (a).
[285] DPA, s 26 (b).
[286] DPA, s 26 (c).
[287] DPA, s 26 (d).
[288] DPA, s 26 (e).
[289] DPA, s 29 (a).
[290] DPA, s 29 (b).
[291] DPA, s 29 (c).

Data subjects are entitled to be notified of any breach of their personal data. Data controllers are required to communicate in writing to a data subject of any access or acquisition by an unauthorized person, especially where the data subject is likely to suffer harm as a result of the breach.[292] The notification should be accompanied by adequate information to enable the data subject protect themselves, and mitigate foreseeable prejudicial impacts of the breach.[293] The qualifier of it posing a real risk of harm is however subjective and may be prone to abuse by data controllers.

The consent granted by the data subject to process data ought to be freely given can be withdrawn at any time.[294]In cases of a minor, the Act prescribes additional safeguards which are aimed at protecting the nest interests of the child[295]. This includes verification of age and consent which are determined on the basis of factors such as the possibility of harm to the child arising from processing of the data[296].

Restrictions of processing of data:

It is evident that processing of data is limited where the accuracy is in question[297], the personal data is no longer required[298], the processing is unlawful[299] and no consent or authorization has been obtained[300] save for the exceptions contained under the Act[301]. It therefore follows that any

[292] DPA, s 43 (1) (b).
[293] DPA, s 43 (5).
[294] DPA, s 32.
[295] DPA, s 33 (1).
[296] DPA, s 33 (3) (d).
[297] DPA, s 34 (1) (a).
[298] DPA, s 34 (1) (b).
[299] DPA, s 34 (1) (c).
[300] DPA, s 34 (1) (d).
[301] DPA, s 30 (1) (b).

data processing that contravenes the states restrictions can constitute an offence, which has largely been the case for offences under both KICA and CMCA.

Institutions established under the Act:

Office of the Data Protection Commissioner

The DPA establishes the Office of the Data Protection Commissioner (ODPC)[302] which has the overall mandate of overseeing the implementation of the Act. The ODPC is tasked with exercising oversight on data processing operations and assess whether information is being processed in compliance with the Act. It is also mandated to process complaints about alleged infringements of rights provided for under the Act.

In addition, the ODPC is also tasked with promoting international cooperation which includes ensuring compliance with international obligations on data protection as well as cooperating with other States on data protection matters.

The inaugural Data Commissioner was appointed on 16th November, 2020. The ODPC has since then established several guidelines to facilitate undertaking their mandate as well as operationalization of the Act. The manuals include the following: Guidance note on consent[303] which outlines obligations of institutions in relation to obtaining consent from data subjects; ODPC data protection impact assessment[304] which offers a guideline which institutions can utilise to

[302] DPA, s 5.
[303] ODPC, *Guidance Note on Consent* (Government Printer, 2020).
[304] ODPC, *Guidance note on Data Protection Impact Assessment* (Government Printer, 2020).

undertake their data protection impact assessment; Huduma Namba Regulations, 2021[305] and the ODPC Complaints Management Manual[306] which provides a step by step guide on processing of complaints.

The ODPC has also developed an online reporting framework whereby a complaint can be filed and data breaches can be reported[307]. Further through the online platform on the ODPCs web page they intend to publish a register of data controllers[308] and data processors[309], however, it has not been implemented.

Investigation and Prosecution under the Act:

The powers granted to the Data Commissioner under the Act bestow investigative, prosecutorial and judicial authority. The Data Commissioner can conduct investigations[310], issue summons[311], facilitate use of alternative dispute resolution mechanisms[312] as well as impose administrative fines[313].

The benefit of conferring investigative, prosecutorial and judicial authority on the Data Commissioner is that those functions shall be carried out by an officer well versed with the

[305] The Registration of Persons (NIIMS) Rules, 2020.
[306] ODPC, *Complaints Management Manual* (Government Printer, 2020).
[307] ODPC, 'Report a Data Breach' (*ODPC*, June 2021)<https://www.odpc.go.ke/report-a-data-breach/>accessed 24 November 2021.
[308] ODPC, *Guidance Note On Registration Of Data Controllers And Data Processors* (Government Printer, 2020).
[309] Ibid.
[310] DPA, s 9(1) (a).
[311] DPA, s 9(1) (d).
[312] DPA, s 9(1) (c).
[313] DPA, s 9(1) (f).

technical knowledge necessary to not only investigate and prosecute but also the specialized technical knowledge to adjudicate a dispute under the Act.

Conclusion

The discussion in this chapter has confirmed the existence and prevalence of cybercrime in Kenya which has largely been correlated to the increased utilization of the internet and ICT and enhanced by automation during the Covid-19 era. It has also provided a background on the countermeasures put in place to address cybercrime in Kenya especially through reliance on the existing cybersecurity institutional and legal framework.

The analysis of the existing legal framework has further highlighted the difference in imposition of penalties which largely appear to be more stringent in the CMCA save for the one imposed on cyber terrorism. It has also linked the actions relating to the said offences and what qualifies them as offences in the first place. The discussion therefore creates a baseline for examining its effectiveness and testing the relevance of both the deterrence and situational crime prevention theories to this study in the next chapter.

CHAPTER THREE: EFFECTIVENESS OF THE CYBERSECURITY LEGAL FRAMEWORK IN ADDRESSING CYBERCRIME IN KENYA

3.0 Introduction

In the preceding chapter we discussed an overview of the cybercrime status in Kenya *vis* a *vis* an analysis of the countermeasures put in place to address cybercrime. Notably both legal and institutional measures are being implemented to safeguard the country from cybercrime. This chapter therefore furthers the study of the phenomenon of cybercrime in Kenya with a view to assessing the effectiveness of the legal framework in countering cybercrime. It will also consider the existing legal provisions and their role in preventing or deterring crime as propagated under the deterrence and situational crime prevention theories considered in the preliminary chapter of this study.

3.1 Theoretical Considerations

Deterrence Theory

The deterrence theory is premised on its ability to not only punish criminal violators through punishments but to also discourage others from committing similar offences. Ceasare Beccaria posits that laws are put in place to support a unified society through their ability to punish violators as well as to deter others from committing similar offences by imposing punishments which are proportionate to crimes committed and they should be immediate, certain and severe[314].

[314] Ben Johnson (n 41) 5.

In similar vein, Jeremy Bentham also urges that human beings are governed by pain and pleasure which motivate their actions. As a consequence, imposing certain, intense and severe punishment for commission of offences would limit pleasure while increasing pain thus making it less desirable to commit the said offences.

Both Beccaria and Bentham posit that imposition of punishments for commission of crimes will have the effect of limiting their perpetuation based on fear by would be criminals. They presuppose that this would be due to their fear of being subjected to the punitive punishments which far outweigh the benefits they would realize from committing the crimes. The deterrence theory is composed of three components which together contribute to making the cost of commission of an offence to far outweigh the benefits of its commission. An effective cybersecurity legal framework would therefore need to have provisions that mirror the three components of the deterrence theory; certainty, celerity and severity.

The *certainty* of the offence makes it likely that an offender would be apprehended, its *celerity* focuses on the speed of imposition of the punishment which is assumed to be more effective and the *severity* of the punishment which indicates to all that the behaviour is unacceptable and the benefit is minimal compared to the punishment. Criminals are deterred from committing offences where there is a likelihood that they will be caught and that the punishment will be immediate and severe.

KICA provides a framework regulating the information technology and telecommunications sector. It criminalizes sending offensive messages and false information by use of computerized

device,[315] and those found guilty are liable to payment of a fine, serving a jail term or both.[316] Whereas publication of incorrect or offensive data has huge capital impacts on the victim for instance in the case of businesses or organisations , the punishment prescribed is minor which has little impact on corporate motivates cybercriminals. In that sense, the severity component of the punishment is minimal in comparison to the benefits that will accrue to the offender.

In addition, disclosing access codes for an unlawful purpose or to cause prejudice to a person is also one of the offences provided for under the Act.[317] The offence attracts payment of a fine or serving a jail term or both. The component of severity in the punishment prescribed for commission of this offence is also not as severe as the implications it carries with the victim possibly loosing data or information.

Whereas Kenya had a significantly robust cybercrime legal framework since 1998 with the highlight and cybercrime specific legislation coming to effect in 2018 and 2019, statistics by National KE-CIRT/CC which shall be highlighted later in this chapter the disagree with the effect of the legislations on the status of cybercrime.

The reports on phishing attacks[318], web application attacks[319], access and interception attacks[320] among other cybercrimes being perpetuated in Kenya paint a negative picture which is far removed

[315] KICA, s 29.
[316] Ibid.
[317] KICA, s 83Z.
[318] Doreen Wainaninah, 'Kenya ranked easiest target in Africa for cyber attackers' *Business Daily* (Nairobi, 2 September 2020) 8.
[319] Communications Authority of Kenya, *National KE-CIRT/CC Cybersecurity Report* (2020).
[320] Communication Authority of Kenya, *Alert on Disclosure of Personally Identifiable Information (PII) Leading to Sim Card Swap Fraud* (2018).

from deterrence. It actually points to emboldened criminals who are enticed to commit cybercrimes.

Situational Crime Prevention (SCP) Theory

The theory has its roots from earlier times. Aristotle for instance considered the nexus between opportunity and theft while ancient Romans relied on SCP theory interventions such as erecting walls and utilizing construction designs to reduce crime. The theory urges that crimes are motivated by situational factors, where the situational factors are manipulated it makes it impossible to commit the crime.[321]

As a result, it proposes techniques and alternatives aimed at reducing and removing opportunities for offenders to commit crimes.

The Situational Crime Prevention theory focuses on concepts of rationality, specificity, and opportunity in addressing crime prevention. An offender's behaviour is therefore characterized as rational, supported by situational characteristics that enable successful completion of the crime based on the available opportunities. To reduce crime, the SCP theory proposes twenty-five general strategies which incorporate both hard and soft techniques and are categorized to include those which; increase effort, reduce rewards, increase risks, reduce provocations and remove excuses[322]. To address cybercrime, the cybersecurity legal framework would therefore require provisions that incorporate the strategies and techniques envisioned under the SCP theory to curb cybercrimes.

[321] Freilich Joshua and Newman Graeme, 'Situational crime prevention' In Pontell H (ed), *Oxford research encyclopedia of criminology and criminal justice* (Oxford University Press 2017) 5.
[322] Ibid.

Increasing effort techniques such as screening of exits, target hardening, controlled access, deflecting offenders and controlling weapons or tools are proposed as techniques for preventing crime. The Kenyan cybersecurity legal framework has prescribed offences which safeguard against unauthorised access, however there is no requirement, standard or policy consideration made towards compelling users to control access to their computers systems and devices. The legal provisions also mandate NCCCC to develop a training framework to tackle prevention and detection of cybercrimes, but to date no such framework has been developed. As a consequence there is no coordinated training on measures such as target hardening, deflection and controlled access.

Increasing risks techniques have similarly been proposed and ought to be implemented by aiding in natural surveillance, spreading guardianship, decreasing anonymity, utilizing place managers and bolstering formal surveillance. A general lack of awareness on what cybercrimes are and how they are perpetuated has contributed to ineffectiveness of the cyber security legal framework in increasing risks. No guidance notes and standards on cybersecurity practice have been developed by the organ tasked to do so under the CMCA. The delay in operationalizing the 2018 Act through constituting by NCCCC has limited its effectiveness in providing guidance on safe cybersecurity practice. This includes provisions on how to conduct surveillance and reduce anonymity of who accesses computer systems, devices and infrastructure which if implemented would increase risks associated with commission of cybercrimes.

Reduction of rewards as an SCP theory categorisation further proposes techniques such removal of targets, concealment of targets, disruption of markets and identification of property to prevent

crime. The provisions enumerated under the existing cyber security legal framework on cybercrime provide for mechanisms for reduction of rewards where a cybercrime is committed. For instance, under the CMCA where a person is convicted on a cybercrime charge, the court has authority to grant an order for compensation for loss incurred due to the offence. It further makes provision for orders of confiscation or forfeiture of proceeds or monies accrued due to commission of the crime as well as an order for restitution.

Additionally, reduction of provocations which utilizes techniques such as reducing emotional arousal, lessening frustrations and stress, circumventing disputes, offsetting peer pressure and putting off imitation techniques has similarly been proposed to address crime prevention. Lastly, SCP theory proposes a category dubbed removal of excuses which consists of techniques such as rule setting, notification of instructions, conscience alerting, assisted compliance and controls is also proposed as a mechanism for prevention of crime and its reduction.

Whereas the legal framework addressing cybercrime in Kenya has provided for mechanisms incorporating the SCP theory such as the need to develop standards on cybersecurity and undertaking awareness and training.

The SCP theory technique on denial of benefits as a way of preventing crime has also been incorporated into the existing legal framework addressing cybercrime in Kenya. Courts are empowered to issue orders for; confiscation, surrender of monies or proceeds as well as assets purchased or obtained by proceeds derived for commission of an offence under the CMCA. [323]

[323] CMCA, s 44 (1).

The inclusion of the techniques in the legal framework should ideally reduce opportunities for the commission of cybercrime and increase risks associated with commission of the crimes due to existence of a more aware target population. However, the inverse is happening, cybercriminals are not deterred from committing cybercrimes despite existence of the risks which are tied to punitive punishments and the prospect of not enjoying the fruits of their 'labour' due to denial of benefits. .

3.3 Impact of the Cybersecurity Legal Framework in Addressing Cybercrime in Kenya

Campaigns on security tips have gained traction in Kenya with most mobile lending telecommunication companies and traditional banks urging their customers not to disclose their passwords[324]. This points to the challenges of cybercrime which have been perpetuated in part by offenders who dupe unsuspecting individuals to disclose their passwords or other personal information which is subsequently used to access accounts and transfer or withdraw funds without the individual's consent[325].

The personal information disclosed to the offenders have been used to access financial institutions such as banks and mobile money applications such as MPESA to illegally and unlawfully withdraw money from the unsuspecting members of the public. The financial loss is not the only end game as the cybercriminals have also utilized information gained to fraudulently disable access and control of bonafide sim card holders to their registered sim cards.

[324] GT Bank, 'Safeguard your account' (*GT Bank*, June 2021) < https://www.gtbank.co.ke/security-centre/security-information> accessed 12 November 2021.
[325] BBC, 'Phone Scam: How Kenyans are losing money' *The Standard* (Nairobi, June 6 2018) 11.

The SIM card swap is one of the crimes which has gained traction in Kenya over the recent past. It is perpetuated by a cybercriminal/ fraudster who calls the target pretending to be an employee of a mobile money operator who asks the target for personal identifiable information and ends up swapping the SIM card and gaining access to all services accessed through it[326]. Often, the target ends up losing money to the cyber criminals who disable the victims' access to their devices and SIM services while regenerating passwords causing financial loss to the targets[327].

Whereas the crime can be committed by any cybercriminal, some instances have been linked to employees of the mobile telecommunications companies who dupe unsuspecting targets to input codes which disable their access or enable transfer of funds illegally from the target's accounts to other stolen SIM cards[328].

The intrusion carried out through the SIM card swap classifies as unauthorized access[329] with intent to commit further offence[330], unauthorized interference[331] and unauthorized interception[332] all of which are punishable cybercrimes under the CMCA and carry punitive punishments including payment of fines and imprisonment in jail. These punishments notwithstanding, instances on the SIM card swap continue to increase in Kenya, bringing to question the efficacy of the legal framework in addressing the crime.

[326] Communications Authority of Kenya (n 319).
[327] Communication Authority of Kenya (n 320).
[328] Jemimah Mueni, '21 year old MPESA and IEBC Systems Hacker arrested by DCI' *Capital FM News* (Nairobi, 17 July 2021) 12.
[329] CMCA, s 14.
[330] CMCA, s 15.
[331] CMCA, s 16.
[332] CMCA, s 17.

Phishing attacks have similarly grown to be the new norm in Kenya. Cybercriminals send emails under the guise of genuine institutions or websites with the ill intention of obtaining unauthorized credentials of the unsuspecting targets. Upon obtaining the credentials, the cybercriminals use them to gain access to the devices of their victims and information therein. The cybercriminals have also used phishing attacks to share malicious links which enable them to obtain credentials such as passwords or PINs[333] later used for an array of malicious operations including unauthorized funds withdrawal and sharing of personal or corporate data without authorization of the affected party.

According to the National KE-CIRT/CC, between October and December 2020 cybercriminals used domain spoofing to create emails. The emails appeared to have originated from Microsoft Outlook and misled unsuspecting targets to click links from fake pages. The cyber criminals thereafter could obtain the credentials of the unsuspecting cyber space users[334]. They also reported that cyber criminals utilized perceived 'special offers' during holiday seasons to dupe unsuspecting members of the public to key in their personal credentials which the criminals later used for unauthorized uses.

As a mitigation measure for containment of Covid-19, many businesses and institutions shifted to remote working, the National KE-CIRT/CC also recorded an increase in spoofing incidents especially for login and download pages for web conferencing platforms such as Skype, Zoom and WebEx[335]. These cybercrimes were being perpetuated despite existence of the cybersecurity legal

[333] Communications Authority of Kenya (n 319).
[334] Ibid.
[335] Ibid.

framework which allows for their detection and prevention even before they happen and their investigation and prosecution thereafter.

The offence of Phishing attracts a jail term, the payment of a fine or both.[336] Nonetheless, the occurrence of phishing attacks has increased in Kenya. The punishments have either lost their deterring effect or they are not stringent enough to pose a risk to the perpetrator who considers the rewards more lucrative than a conviction which would affect their freedom or impact on their finances.

Malware attacks have similarly been reported to be increasing in Kenya, with a 44.7% increase being recorded by the National KE-CIRT/CC between October and December 2020 where they recorded forty-six million, sixty-nine thousand, five hundred and twenty-five (46,069,525) malware threat events[337]. Malware attacks refer to the use of malicious code or programs which may include viruses, bugs, works, spyware, rootkills, adware, trojans or even ransomware with the intention of getting unauthorized control of a system or device[338]. This has also shifted from commonly affected systems or computers to mobile devices which are targeted by malicious applications which appear as original applications in the device applications stores. Malware attacks have also been perpetuated to steal information and harvest it from devices or systems without the consent of the affected party.

[336] CMCA, s 30.
[337] Communications Authority of Kenya (n 319).
[338] Ibid.

Commission of malware attacks equates to commission of cybercrimes such as unauthorized access and interception[339] which may be used to not only harvest data from a targets device or system but may also be used to destroy or misdirect the data.[340] A person found culpable of committing malware attacks is liable to payment of a fine or serving a jail term or both.

A person convicted for wilful misdirection of electronic messages is liable to payment of a fine or serving a jail term or both.[341] This notwithstanding, the National KE-CIRT/CC recorded an almost half increase in malware attacks at the end of the year 2020.

Notably, there has been a similar increase in web application attacks which have increased by a whopping 281.4% to a total of seven million, eight hundred and forty-seven thousand, four hundred and fifty-seven (7,847,457) between the period of October to December 2020 as compared with a similar timeline between July and September 2020[342]. This prevalence has been attributed to increased use of online platforms which are unsecured, a lack of awareness or technical capacity to properly secure them as well as a failure to update plug-ins.

The web application attacks have created an avenue for cyber criminals to install applications such as payment skimmers, to crash the targeted sites as well as to retrieve information without authorization to the detriment of the target. The compromising of devices and systems through web application attacks provides an avenue for commission of cybercrimes yet the CMCA is only

[339] CMCA, s 31.
[340] CMCA, s 32.
[341] Ibid.
[342] Communications Authority of Kenya (n 319).

treating its resultant effects such as unauthorized access, unauthorized interception without addressing web application attacks as a cybercrime in itself.

Distributed Denial of Service (DDoS) cyber-attacks are used to undertake malicious disruptions of normal traffic by overwhelming the targeted server or its supporting information technology infrastructure with a barrage of internet traffic[343]. DDoS attacks like other cyber-attacks have also increased drastically in Kenya, with a recorded increase of 81.5% between October and December 2020 at two million, two hundred and sixty thousand and thirty-six (2,260,036) from those recorded between the period July to September 2020[344].

Investigations relating to cybercrimes have as consequentially also gained momentum. The National KE-CIRT/CC recorded an increase between October and December 2020 of forensic investigations undertaken by their Digital Forensics Lab (DFL) which increased to fifty-eight (58) as opposed to fifteen (15) requests carried out between July and September 2020[345].

The increase in requests was largely attributed to increased and unsupervised exposure of children to mobile devises over the long school closure period as a mitigating measure for addressing Covid-19[346]. The increase in investigations points to the influence of an elaborate framework which classifies and prescribes cybercrime offences, yet it does not even slightly mirror the increase in perpetrated cybercrimes. This therefore begs the question does the legal framework aid

[343] Ibid.
[344]Ibid.
[345] Ibid.
[346] Ibid.

investigations of cybercrimes or it works against it based on the inconsequential number of investigations in comparison to the cybercrimes undertaken within the same period.

Conclusion:

The cyber security legal framework though lauded for its elaborate provisions, seems to have made a small dent in the fight against cybercrime in Kenya. Whereas investigations on cybercrime have gone up, there is little to no data on the prosecution rates for the investigations that give rise to commission of a cybercrime offence. Further, there is even scantier information on the conviction rates for cybercrimes by mainstream government with only limited information being captured in news reports and other technology company reports.

On the other hand, the prevalence of cybercrime has gone up based on quantifiable reports issued by the National KE-CIRT/CC which is mandated to coordinate responses to cybersecurity incidents in Kenya. The existing cybersecurity legal framework has therefore failed in not only deterring cybercrime but it also appears to have significantly failed to tilt the scales on preventing cybercrime and has instead continued to foster opportunities for its commission based on the rising trends.

CHAPTER FOUR: FINDINGS, CONCLUSIONS AND RECOMMENDATIONS

4.0 Introduction

This paper essentially assesses the efficacy of the cybersecurity legal framework in addressing cybercrime in Kenya. This was undertaken through an exploration of the current cybercrime status in Kenya, a review of the existing cybersecurity legal framework and its impact in addressing cybercrime. The researcher was prompted to focus on this particular topic due to the fast pace individuals and institutions have embraced use of the internet and ICT in service delivery which has had a corresponding impact on cybercrime which has similarly increased.

Following prevalence of the Covid-19 pandemic it was necessary to have more automated service provision and remote working. This resulted in more users shifting their business models to use of the internet and ICT's to ensure continuity in service delivery. As a result, the target base for cyber criminals has also significantly increased but with parties who are considerably less cyber risk averse due to their limited interaction within the cyberspace.

Consequentially, it has become necessary to interrogate whether the existing cybersecurity legal framework can protect the "new" users of the cyberspace from falling as prey to cybercrimes if the statistics on cybercrime increase are anything to go by. This paper interrogated the issues with particular focus on the current status of cybercrime in Kenya, analyse the existing cybersecurity legal framework which addresses cybercrime with a view to assessing its efficacy. This chapter will therefore outline summarily the findings of the research while considering their impact on the hypotheses, propose recommendations and conclude the study.

4.1 Findings of the Study

To interrogate the efficacy of the cybersecurity legal framework in addressing cybercrime in Kenya, the researcher framed three research questions which this study sought to respond to. The status of cybercrime in Kenya was discussed in chapter two which confirmed the existence of cybercrime in the country and established that it has continued to evolve over the years in technique as well as frequency.

The increase in cybercrimes was largely attributed to the integration of ICT and use of the internet in service delivery in the last decade and most recently as a Covid-19 pandemic mitigation measure. Notably, aside from the electronic transactions by banks and mobile money operators, the Government had also shifted to offering e-Government services through platforms including the NEMIS[347], KUCCPS[348], iTax[349], IFMIS[350], TIIMS and e Citizen.

Other institutions such as the Judiciary fully embraced use of ICT and the internet after the Covid -19 pandemic when they adopted use of virtual hearings[351]. The integration of ICT and the internet in service delivery had tremendous benefits for most of the institutions including KRA which

[347] This is a web based data management system used to collect data from different education institutions to enhance decision making and planning in the education sector. It collects data on schools and learner information and enables education agencies to share collected information online.
[348] It is an online based platform which allows students to apply online for government placement in Kenyan universities and Colleges.
[349] This is an online service area administered by the Kenya Revenue Authority (KRA) where KRA pin holders can access services remotely.
[350] It is a web based integrated system which allows users both from National and County Government to plan their budgets, procure, reconcile revenue and payments and report on the financial situation.
[351] The Judiciary, Republic of Kenya, *Practice Directions for the Protection of Judges, Judicial Officers, Judiciary Staff, Other Court Users and The General Public From The Risks Associated With The Global Corona Virus Pandemic* (Government Printer, 2020).

widened its tax base and collected more revenue[352] and the Ministry of Education enhanced its capacity to track students and plan for schools through the NEMIS platform[353] to name a few.

Whereas the benefits of automation are significant, the challenges that were brought to the fore in the form of cybercrime cannot be gainsaid. Commission of cybercrime offences has not only resulted in financial loss but has also infringes on constitutional right to property and privacy.

In an attempt to counter the foregoing challenges legal and institutional reforms have been put in place. Kenya has enacted three laws which safeguard processing of personal data as well as prescribe cybercrime offences and punishments for their commission.

KICA was the first law enacted to regulate the information, communication and technology sector. The following cybercrime offences and their punishments are prescribed under the Act; improper use of a system, disclosure of access codes for an unlawful purpose, reprogramming of mobile telephones, unlawful modification or interference with messages, willful tampering with telecommunication apparatus for unlawful use and publication of obscene information.

The Act empowers authorized persons by the Communication Authority in conjunction with police officers to undertake searches for purposes of investigations under the Act. Further, authorized officers of the Communication Authority are also empowered to prosecute offences under the Act.

[352] Dennis Onsongo (n 4) 5.
[353] Global Partners for Education, 'A New Web-Based Tool Is Poised To Transform Education Management And Delivery in Kenya' (GPE, July 2017)<https://www.globalpartnership.org/blog/new-web-based-tool-poised-transform-education-management-and-delivery-kenya > accessed 2 July 2021.

The Act establishes several institutions including the Communication Authority which constituted the National KE-CIRT/CC to support its mandate on responding to cybersecurity issues.

The second legislation discussed in chapter two is the CMCA which is the first legal framework of its kind in Kenya that provides a framework for curbing cybercrimes. Whereas the Act faced operationalization hurdles which have only recently been cleared up by the Court of Appeal and through administrative action of constituting the NCCCC, it remains significant in discussions on cybercrime in Kenya.

The Act prescribes several cybercrime offences as well as their corresponding sanctions, which is more elaborate and carries enhanced punishments. It prescribes the offence of forgery through a computer medium, fraud committed in the cyberspace, cyber harassment, cybersquatting, identity theft or impersonation, cyber terrorism, false publication and intentional withholding of electronic mail, payments and debit or credit cards.

The Act further prescribes an offence relating to failure to disclose cyber intrusions or attacks within 24 hours and creates a leeway for prosecution of other offences which are committed through a computer. Similar to KICA, the Act also empowers cybersecurity experts appointed by the Cabinet Secretary responsible for National Security to undertake investigations through search and seizure. The Act further creates a framework for international cooperation through mutual legal assistance which is cognizant of the nature of cybercrimes since they can be committed across territorial boarders of more than one State.

The DPA was also interrogated in the study. It provides a framework on how personal information should be processed. It also outlines the data subject's right to notification of the indented use of the data and the right to consent or decline to its processing. It also establishes the ODPC that is primarily tasked with supervising implementation and enforcement of the Act. Following the appointment of the inaugural Data Commissioner under the office, considerable milestones have been achieved such as development of a guidance note on consent which is crucial in safeguarding the right to privacy and in enhancing informed choices on giving or withholding consent.

The consideration of the status of cybercrime in Kenya and subsequent analysis of the existing cybersecurity legal framework addressing cybercrime revealed that cybercrimes stills persisted and had become more prevalent during the same duration. This was despite existence of the legal and institutional framework which is fairly elaborate in its provisions ranging from prescribing cybercrime offences and punishments for their commission, establishing reporting frameworks to track cyber incidents, provisions for securing evidence, delegation of prosecutorial powers, provision for mutual legal assistance and prescribing for provision of training on cybersecurity measures.

In support of this assertion, the National KE-CIRT/CC prepared a report that indicated a total of 158,405,656 cyber threats were detected within the financial year 2020/2021 out of which 38,776,699 were those recorded between April and June 2021[354].

[354] Communications Authority of Kenya (2021), *Quarter Four, National KE-CIRT/CC Cybersecurity Report April to June 2021* p. 6.

Notably, all three of the Acts of Parliament enacted to address cybercrime were in existence and two out of the three were fully operational, that is KICA and the DPA.

Chapter three of the paper responded to the third and final research question on whether the existing cybersecurity legal framework was effective in addressing cybercrime in Kenya. The impact of the legal framework was considered in relation to the theoretical framework. Whereas the Acts prescribed specific offences and enhanced punishments, they had limited impact in deterring cybercrime which continued to be committed in larger proportions.

It was also established that whereas the Situational Crime Prevention theory advocated for manipulation of circumstances to curb cybercrime, limited interventions in the form of public awareness and training by institutions obligated to undertake the same or development of cybersecurity standards was undertaken.

The study established that prevalence of cybercrimes has been attributed to poor cyber hygiene as a result of unsecured platforms or a general failure to update plug-ins. The increase in commission of cybercrimes in Kenya has also been credited to lack of awareness and limited technical capacity to secure computer systems and platforms.

Further, the study established there is a gap between detection and investigation of cybercrimes. Whereas the cyber threats detected are high in number requests for forensic investigations are considerably low. Resultantly this factors have done little to combat cybercrime which has instead been on the rise despite existence of the legal framework. The chapter therefore also conclusively

highlighted the challenges which have impeded the efficacy of the existing cybersecurity legal framework in addressing cybercrime in Kenya.

4.2 Importance of the Findings

The cybersecurity legal framework currently in place is significant in addressing cybercrime in the Country since it not only prescribes offences and punitive punishments but it also proposes policy reforms to address cybercrime such as development of standards and facilitation of awareness.

It further provides a framework for international cooperation with other States to ensure cyber criminals are subjected to the full force of the law without limitations on jurisdictional issues. Additionally, it provides a framework for denial of benefits of proceeds emanating from commission of cybercrimes which ought to have the impact of making cybercrime a less attractive crime to commit.

The findings of this study are important since they reaffirm the researchers' hypotheses that increased automation of services and proliferation of the use of the internet and ICT has exposed individuals and organisations to cybercrime. Further that cybercrime has consequentially become prevalent due to the increased automation and despite existence of a cybersecurity legal framework addressing cybercrime.

Secondly, the findings of this study are significant because they expand the body of research on cybercrime which was previously limited to sectoral considerations specifically electronic transactions by banks and operations of telecommunication companies. This study expands the

scope to include e-Government services from diverse sectors. Additionally, the focus on Kenya was important to highlight issues that are peculiar to Kenya alone without generalizing to other countries. As a result, the strengths and weaknesses of the legal framework can easily be outlined from the study.

The findings also review the cybersecurity legal framework in light of the deterrence theory and situational crime prevention theory which are key criminal theories and are significant in addressing cybercrime. The consideration of the two theories has pointed out the gaps that contribute to prevalence of cybercrime therefore offering areas for possible recommendations to improve efficiency of the existing legal framework in addressing cybercrime.

Overally, the study has established that whereas the existing legal framework is not perfect, it largely suffers for delay in its operationalization which has hindered its ability to efficiently address the growing concern of cybercrime in Kenya.

4.3 Recommendations

To combat cybercrime and improve the efficacy of the existing cybersecurity legal framework in addressing cybercrime, the researcher proposes the following recommendations;

1. **Holistic implementation of existing legislation; the CMCA and the DPA.**

   Slow operationalization of the both Acts of Parliament limited the ability to tackle cybercrime in Kenya. The institutions and offices which are key in facilitating the purpose

of the Acts have slowly been operationalized, the ODPC was operationalized in November 2020 while the NCCCC was constituted in November 2021.

2. **Sensitization on cybersecurity and cybercrime.**

   Lack of awareness has been a significant impediment to the fight against prevalence of cybercrime due to the lack of cyber hygiene exhibited by individuals and organisations which renders them vulnerable for cyber attacks.

   The NCCCC should develop a framework and roll out a sensitization campaign on cybersecurity, cybercrime and how to protect themselves from being victims.

   The Government should partner with the private sector in activities such as the annual Africa legal hackathon and other cybersecurity campaigns being implemented in the country to enhance awareness on cybersecurity and cybercrime.

3. **Develop localised expertise on cybersecurity, detection techniques, investigation and prosecution of cybercrime as well as response to cyber threats and cybercrimes.**

   Whereas detection of cyber threats is fairly high, the investigations and eventual prosecution rates are significantly low. This gap in the criminal justice framework has been attributed to the limited capacity to handle cybercrime thus contributing to emboldening cybercriminals in the absence of lessons on punitive measures that would be meted for commission on cybercrimes.

The State should therefore facilitate specialised training for law enforcement officers as well as justice sector players such as prosecutors with the ODPP, State Counsel in the OAG and judicial officers on emerging cyber threats, modern mitigating techniques and new detection techniques, investigation and prosecution of cybercrime.

4. **Promote information and knowledge sharing to enhance real-time communication of cyber threat information.**

Whereas disclosure of cyber threats is required to be done within 24hours, it is necessary for the relevant law enforcement agencies to collaborate in a timely manner to information availed on the cyber threats. This can enable them to foil other anticipated attempts as well as provide valuable information on emerging cybercrimes which would in turn influence the sensitization and trainings to be carried out as well as the standards or guidance notes to be developed to address cybercrime.

The NCCCC should collaborate with relevant state agencies both locally and internationally through the mutual legal assistance framework on addressing threats of computer and cybercrime incidents.

The ODPC to fastrack mapping and registering of data controllers and data processors thus creating an available repository for tracking data breaches if any.

The NCCCC should leverage on the reports published by the National KI-CIRT/CC to initiate and coordinate the scrutiny of cyber threats and response to cyber incidents threatening the Kenyan cyberspace.

The Government to collaboratively develop a framework to link the NCCCC, the National KE-CIRT/CC, the DCI unit on cybercrime, the ODPC, the ODPP and the OAG for efficient and real time information sharing on cybercrimes and cyber threats.

5. **Formulation of standards and guidance notes.**

The limited development of guidance notes and standards on promoting cybersecurity have impacted on the capacity of institutions to address cybercrime in Kenya. The NCCCC should therefore develop codes and standards of cybersecurity practice to not only guide owners of critical national information infrastructure but also provide an overall framework for institutions.

6. **Enhance capacity to respond to cybercrime through improved infrastructure for forensic analysis of evidence.**

The Digital Forensic Lab of DCI located in Nairobi has been the sole centre for undertaking forensic investigations relating to cybercrimes, this may therefore impact on the ability to fastrack investigations.

When it is overloaded with requests for investigations from across the country as well as those arising from requests under the mutual legal assistance framework. It is therefore

necessary for the Government to commission development of additional digital forensic labs to supplement the existing DCI Digital Forensic Lab to fastrack analysis of evidence collected relating to commission of cybercrimes. Improved infrastructure will also enhance capacity of investigators to respond to cybercrime through prosecution backed properly processed and admissible evidence.

7. **Improve Cyber-hygiene.**

   Poor cyber-hygiene has been highlighted as one of the challenges contributing to the prevalence of cybercrimes. Training and implementation of proper cyber-hygiene techniques such as frequent cyber risk checks on systems to ensure proper security measures are in place such as access codes, frequent changing of access codes and introduction of levels of access for confidential or sensitive information and secure access to sites should be encouraged for institutions as well as individuals.

8. **Champion for reporting of cybercrimes and cyber threats.**

   There is a knowledge gap on the number of cybercrimes reported and their status whether they resulted in prosecution of offenders and culminated in convictions. Effective reporting of cybercrimes and cyber threats by victims is therefore key to deterring commission of cybercrimes as potential cyber criminals would be wary of subjecting themselves to punishment they see others being subjected to. Further, reporting of cybercrimes will facilitate prosecution of cybercrimes which can only be initiated after a report is lodged and investigated.

9. **Promote research to spur technological innovations to address cybercrime.**

   Limited research on cybercrime in Kenya and globally has significantly impacted on the capability of Countries to tackle cybercrime based on evidence based proposals. Promotion of research will therefore provide an avenue for innovativeness in addressing cybercrime as more scholars will propose research based mechanisms and techniques to address the menace.

4.4 Proposals for Further Research

In view of the study findings, further study on the following topics is recommended:

1. Efficacy of the NCCCC in combating cybercrime in Kenya. This study would evaluate the impact of the Committee in addressing cybercrime, noting that it was less than a month old at the time this study was finalised.

2. The Nexus between Cybersecurity Awareness and Prevalence of Cybercrime in Kenya. This study would specifically consider whether there is a causal link between lack of awareness on cybersecurity matters and prevalence of cybercrime.

4.5 Conclusion

The fast embracing of information, communication and technology as well as the internet in most facets of day to day life has improved service delivery. It has, however, also exposed users of the cyberspace to cybercrimes. Their exposure to cybercrimes has been aggravated by a failure of the State to wholly implement its existing legal framework on cybercrime; undertake sensitization campaigns and trainings; improve infrastructure and encourage reporting. The efficacy of the

cybersecurity legal framework can however be salvaged if implemented correctly and the recommendations proposed are implemented by the relevant agencies.

BIBLIOGRAPHY

Books and Book Chapters

1. Freilich Joshua and Newman Graeme, 'Situational crime prevention' In Pontell H (ed), *Oxford research encyclopedia of criminology and criminal justice* (Oxford University Press 2017) 5.
2. Khushal Vibhute and Filipos Aynalem, *Legal research methods: Teaching material* (The Justice and Legal System Research Institute, 2009) 23.

Conference/Discussion/ Working Papers

1. Ben Johnson, 'Do Criminal Laws Deter Crime? Deterrence Theory in Criminal Justice Policy: A Primer' (2019) MN House Research Department.
2. Enrico Calandro and Nils Berglund, 'Unpacking Cyber-Capacity Building in Shaping Cyberspace Governance: the SADC case' (GIGAnet Conference Paper, annual symposium, Berlin 2019).
3. ICPAK, 'The benefits, challenges and way forward of IFMIS in Kenya' (IPSAS Workshop, 27th-28th June 2017, Merica Hotel, Nakuru).
4. Kate Bowers, Shane D. Johnson and Alex FG Hirschfield, 'Closing off opportunities for crime: An evaluation of alley-gating' (2004) 10 (4) European Journal on Criminal Policy and Research 285, 290.
5. Kwasi Adomako, Nabeel Mohamed, Aminata Garba and Martin Saint, 'Assessing cybersecurity policy effectiveness in africa via a cybersecurity liability index' (2018) Department of Electrical and Computer Engineering Carnegie Mellon University, Kigali, Rwanda.

6. Nicole Beebe and Srinivasan Rao, ‘Using situational crime prevention theory to explain the effectiveness of information systems security’ (The 2005 SoftWars Conference, Las Vegas, November 2005).
7. Rick Brown and Nicola Billing, ‘Tackling car crime: An evaluation of sold secure’ (1996) Paper 71 Crime Detection and Prevention Series, Home Office Police Research Group.
8. Robert Potter and Paul Thomas, ‘Engine immobilisers: how effective are they’ (2001) National CARS project, Adelaide, Australia.
9. Schreuder Cliffe and Mohammad Shan et al, ‘Needs assessment of cybercrime and digital evidence in a UK police force’ (2018) CARI Project, The Cybercrime and Security Innovation (CSI) Centre Leeds Beckett University.
10. Valdemar Sousa, ‘A Review on Cyber Attacks and Its Preventive Measures’ (The Digital Privacy and Security Conference, 2019, Lusofona University of Porto, Portugal).

Guidelines, Policies and Procedures

1. Communication Authority of Kenya (2020), *General Information Security Best Practice Guide*.
2. ODPC, *Complaints Management Manual* (Government Printer, 2020).
3. ODPC, *Guidance Note on Consent* (Government Printer, 2020).
4. ODPC, *Guidance note on Data Protection Impact Assessment* (Government Printer, 2020).
5. ODPC, *Guidance Note On Registration Of Data Controllers And Data Processors* (Government Printer, 2020).

Journal Articles

1. Anna Leppänen, , Tero Toiviainen and Terhi Kankaanranta, 'From a Vulnerability Search to a Criminal Case: Script Analysis of an SQL Injection Attack' (2020) 14 (1) International Journal of Cyber Criminology 63, 65.
2. Benson Muriuki, 'Factors Contributing to Cyber Security Framework In Kenya: A Case Study of Kenyan Telecommunications Companies' (2018) 6 (3) Global Scientific Journals 156.
3. Charles Ishengoma, 'Legal framework challenges to e-banking in Tanzania' (2019) 3 (2) PSU Research Review 33.
4. George Okello and Joseph Ntayi, 'Mobile money adoption and usage and financial inclusion: mediating effect of digital consumer protection' (2020) 22 (3) Digital Policy, Regulation and Governance Journal 14.
5. Hassan Younies and Tareq Na, 'Effect of cybercrime laws on protecting citizens and businesses in the United Arab Emirates (UAE)' (2020) 27 (4) Journal of Financial Crime 1089, 1092.
6. Kadima Chitechi, Samuel Mungai Mbugua and Kelvin Omieno, 'Facilitating factors for cybersecurity vulnerabilities in Kenyan county governments' (2018) 2 (1) Asian Journal of Research in Computer Science 1, 3.
7. Kofi Koranteng and Emmanuel Adjei, 'The phenomenon of data loss and cyber security issues in Ghana' (2018) 20 (2) Foresight Journal 150, 151.
8. Maria Bada, Basie Von Solms and Ioannis Agrafiotis, 'Reviewing National Cybersecurity Awareness for Users and Executives in Africa' (2019) 12 (1) International Journal on Advances in Security 108.

9. Mittal, Sandeep, and Prof Sharma, ‘A review of international legal framework to combat cybercrime’ (2017) International Journal of Advanced Research in Computer Science 2.
10. Naci AKDEMİR, Bülent SUNGUR,and Bürke BAŞARANEL, ‘Examining the Challenges of Policing Economic Cybercrime in the UK’ (2020) *Güvenlik Bilimleri Dergisi* 113, 114.
11. Nir Kshetri, ‘Cybercrime and cybersecurity in Africa,’ (2019) 22 (2) Journal of Global Information Technology Management 77, 81.
12. Norman Mugarura and Emma Ssali, ‘Intricacies of anti-money laundering and cyber-crimes regulation in a fluid global system’ (2020) 24 (1) Journal of Money Laundering Control 10, 12.
13. Olayinka Akanle and Babajide Richard Shadare, ‘Why has it been so difficult to Counteract Cyber Crime in Nigeria? Evidence from an Ethnographic Study’ (2020) 14 (1) International Journal of Cyber Criminology 29, 31.
14. Sarah Gordon and Richard Ford, ‘On the definition and classification of cybercrime’ (2006) 2 (1) Journal in Computer Virology 13, 15.
15. Sinchul Back and Jennifer LaPrade, ‘Cyber-situational crime prevention and the breadth of cybercrimes among higher education institutions’ (2020) 3 (2) International Journal of Cybersecurity Intelligence & Cybercrime 25, 36.
16. Sylvia Ndanu and Zhang Yanqiu, ‘Online content regulation policy in Kenya: potential challenges and possible solutions’ (2021) 6 (2) Journal of Cyber Policy 177, 180.
17. Uchenna Jerome, ‘Protecting Consumers from Cybercrime in the Banking and Financial Sector: An Analysis of the Legal Response in Nigeria’ (2019) 24 (1) Tilburg Law Review.

18. Valery O. Lutta and John Obiri, 'Cyber Crime a Rising Threat for Internet – Based Businesses in Western Region, Kenya' (2015) 6 (3) International Journal of Scientific and Engineering Research 317, 320.

Newspaper Articles

1. BBC News, 'Kenya Revenue Authority 'Lost $39m to hacker,' *BBC News* (22 March 2017) 4.
2. BBC, 'Phone Scam: How Kenyans are losing money' *The Standard* (Nairobi, June 6 2018) 11.
3. Benjamin Muriuki, 'IFMIS safe and secure, says gov't after 18 websites reported hacked' *Citizen Digital* (Nairobi, 3 June 2019) 11.
4. Bruhan Makong, 'Kenya Unveils National Computer and Cybercrimes Co-ordination Committee to fight Cybercrime' *Capital News* (Nairobi, November 4 2021) 6.
5. Dennis Onsongo, 'How KRA can make the most of its iTax platform,' *The Business Daily* (Nairobi, 16 June 2019).
6. Doreen Wainaninah, 'Kenya ranked easiest target in Africa for cyber attackers' *Business Daily* (Nairobi, 2 September 2020) 8.
7. Frankline, 'Kenyans warned against returning missed international calls' *The Standard* (Nairobi, 11 May 2018).
8. Jemimah Mueni, '21 year old MPESA and IEBC Systems Hacker arrested by DCI' *Capital FM News* (Nairobi, 17 July 2021) 12.
9. Mercy Muendo, 'Kenya's new cybercrime laws open the door to privacy violations, censorship' *The Conversation* (Nairobi, 29 May 2018) 11.

10. Munguti Richard, 'JKUAT students charged with hacking bank, stealing millions' *Daily Nation* (Nairobi, 27 October 2020) 5.
11. Olingo Allan, 'Two Kenyan banks lose $ 0.86 million to hackers in a month' *The East African* (Nairobi, 14 July 2018) 2.
12. Paul Ogemba, 'Man charged with hacking KRA and causing Kenya shillings 4 Billion loss' *The Standard* (Nairobi, 22 March 2017) 6.

Blogs and Websites

1. Council of Europe, 'Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY' (*Council of Europe,* June 2021) <https://www.coe.int/en/web/cybercrime/parties-observers>accessed 22 September 2022.
2. Council of Europe, 'The Budapest Convention on Cybercrime: Benefits and Impact in Practice' (*Council of Europe*, July 2020) <https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac>accessed 22 September 2022.
3. ENISA-European Union Agency for Cybersecurity, 'Emerging Trends from January 2019 to April 2020 Enisa Threat Landscape' (*Enisa,* June 2020) <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-list-of-top-15-threats/at_download/fullReport> accessed 14 January 2021.
4. Global Partners for Education, 'A New Web-Based Tool Is Poised To Transform Education Management And Delivery in Kenya' (GPE, July 2017)<https://www.globalpartnership.org/blog/new-web-based-tool-poised-transform-education-management-and-delivery-kenya > accessed 2 July 2021.

5. GT Bank, 'Safeguard your account' (*GT Bank*, June 2021) < https://www.gtbank.co.ke/security-centre/security-information> accessed 12 November 2021.
6. Lolyne Ongeri, 'LSK challenges the constitutionality of the Computer Misuse and Cybercrimes Act' (*Ifree*, June 2018) < https://www.ifree.co.ke/2018/06/lsk-challenges-constitutionality-of-the-computer-misuse-and-cybercrimes-act/> accessed 20 November 2021.
7. NewZealand Government, 'Situational Crime Prevention: Evidence Brief' (*NewZealand Government*, April 2017) <https://www.justice.govt.nz/assets/Documents/Publications/Situational-Crime-Prevention.pdf> accessed 23 June 2021.
8. ODPC, 'Report a Data Breach' (*ODPC*, June 2021)<https://www.odpc.go.ke/report-a-data-breach/>accessed 24 November 2021.
9. The National Treasury, 'IFMIS Department' (*The National Treasury*, June 2022) <https://www.treasury.go.ke/ifmis/#:~:text=One%20of%20the%20PFM%20reforms,at%20enhancing%20accountability%20and%20transparency.>accessed 30 October 2022.
10. The NATO CCDCE, 'Mixed Feedback on the African Union Convention on Cyber Security and Personal Data Protection' (*CCDCE*, June 2020)<https://ccdcoe.org/incyder-articles/mixed-feedback-on-the-african-union-convention-on-cyber-security-and-personal-data-protection/ > accessed 21 November, 2021.
11. Victoria Wangui, 'Petitioner challenges the Computer Misuse and Cybercrimes Act' (*Ifree*, May 2018)< https://www.ifree.co.ke/2018/05/petitioner-challenges-computer-misuse-and-cybercrimes-act/> accessed 20 November 2021.

Government Reports and Publications

1. African Union, *List of Countries which have signed, ratified/acceded to the AUCCPDP* (Addis Ababa, 2014).
2. Communication Authority of Kenya (2018), *Advisory by the Communication Authority of Kenya (CA) on the Emotet Malware*.
3. Communication Authority of Kenya (2018), *Alert on Disclosure of Personally Identifiable Information (PII) Leading to Sim Card Swap Fraud*.
4. Communication Authority of Kenya (2020), *20 years of Kenya's ICT Progress* Annual report 2019-2020.
5. Communications Authority of Kenya (2020), *National KE-CIRT/CC Cybersecurity Report* (January-March 2020).
6. Communications Authority of Kenya (2020), *National KE-CIRT/CC Cybersecurity Report* (2020).
7. Communications Authority of Kenya (2021), *National KE-CIRT/CC, Cybersecurity Report* (January - March 2021).
8. Communications Authority of Kenya (2021), *Quarter Four, National KE-CIRT/CC Cybersecurity Report April to June 2021)*.
9. Communications Authority of Kenya (2021), *Third Quarter Sector Statistics Report for the Financial Year 2020/2021*.
10. Government Printer, *Annual Report to Parliament on the State of National Security* (Nairobi, March 2020).
11. Serianu (2020), *Local Perspective on Data Protection and Privacy Laws: Insights from African SMEs* Africa Cybersecurity Report Kenya, 2019/2020.

12. The Judiciary, Republic of Kenya, *Practice Directions for the Protection of Judges, Judicial Officers, Judiciary Staff, Other Court Users and The General Public From The Risks Associated With The Global Corona Virus Pandemic* (Government Printer, 2020).

Research Projects

1. Clinton Mwale, 'The Phenomenal Adequacy and Efficiency of Cyber Crime Laws in Kenya' (Bachelor of Laws Dissertation, Moi University, 2017) 6.
2. Sinesipho Ralarala, 'The Impact of cybercrime on e-commerce and regulation in Kenya, South Africa and the United Kingdom' (Master of Laws Thesis, Strathmore University, 2020) 6.