UNIVERSITY of LUSAKA

Passion for Quality Education: Our Driving Force

SCHOOL OF LAW

A COMPARATIVE ANALYSIS OF ENFORCEMENT - RELATED PROVISIONS IN THE DATA PROTECTION ACT IN ZAMBIA WITH THOSE IN COUNTERPART LEGISLATION IN SOUTH AFRICA, KENYA, NIGERIA, AND THE UNITED KINGDOM

BY

MARGARET BANDA

LLB22114013

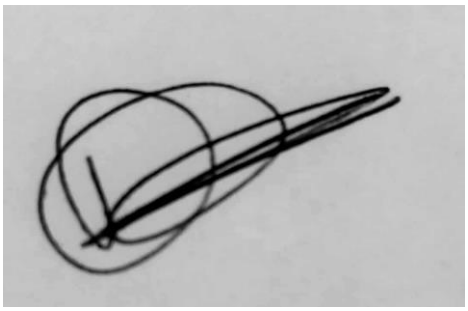
An obligatory essay submitted to the University of Lusaka in partial fulfillment of the requirement for the award of the Bachelor of Laws (LLB) Degree

2025

DECLARATION

I, **MARGARET BANDA,** do declare that this dissertation titled **"A COMPARATIVE ANALYSIS OF ENFORCEMENT-RELATED PROVISIONS IN THE DATA PROTECTION ACT IN ZAMBIA WITH THOSE IN COUNTERPART LEGISLATION IN SOUTH AFRICA, KENYA, NIGERIA, AND THE UNITED KINGDOM"** which is hereby submitted to the School of Law at the University of Lusaka as part of the requirements for the award of the Bachelor of Laws (LLB) degree, is my original work and has not previously been submitted for the award of a degree at this or any other tertiary institution. The sources that have been used or quoted have been indicated and duly acknowledged as complete reference

MARGARET BANDA



2025

SUPERVISOR'S RECOMMENDATION

I, KATONGO CHILESHE, do recommend that this dissertation titled **"A COMPARATIVE ANALYSIS OF ENFORCEMENT - RELATED PROVISIONS IN THE DATA PROTECTION ACT IN ZAMBIA WITH THOSE IN COUNTERPART LEGISLATION IN SOUTH AFRICA, KENYA, NIGERIA, AND THE UNITED KINGDOM"** done under my supervision, be admitted by the university, I have checked it carefully and I am satisfied that it meets necessary requirements pertaining to the format laid down by the university regulations.

Ms. KATONGO CHILESHE

(Supervisor)

……

(Date)

DEDICATION

I dedicate this work to my loving husband Sylvester Mwansa, wonderful children and loving parents, whose patience, understanding and unwavering support made this journey possible.

ACKNOWLEDGEMENTS

First and foremost, I thank God for his mercy, grace and guidance throughout the course of this research, his strength has sustained me from the beginning to the end of this work.

I would like to express my sincere gratitude to my supervisor Ms. Katongo Chileshe for her guidance, constructive feedback and continuous support. Her dedication and expertise greatly contributed to the successful completion of the study,

My appreciation also goes out to my colleagues and peers at law school who contributed to my growth and learning throughout this journey. Thank you for celebrating my progress and reminding me that I will achieve this, your friendship has been a blessing I will always cherish.

Finally I am grateful to all participants and individuals who contributed in various ways to the completion of this research.

TABLE OF CONTENTS

TABLE OF STATUTES

Constitution of the Federal Republic of Nigeria 1999

The Cyber Security Act No. 3 of 2025

The Cyber Crimes Act No. 4 of 2025

The Data Protection Act No. 3 of 2021

Data Protection Act No. 3 of 2021

Data Protection Act No. 24 of 2019

Protection of Personal Information Act No. 4 of 2013

Nigeria Data Protection Act No. 37 of 2023

The United Kingdom’s Data Protection Act, 2018

ABSTRACT

This study compared the enforcement provisions of Zambia's *Data Protection Act No. 3 of 2021* with similar laws in South Africa, Kenya, Nigeria, and the United Kingdom. It focused on how these laws balance strong enforcement with the protection of individual rights. The research found that Zambia's Act gives inspectors wide powers under Sections 7 to 11 to enter premises, seize property, and make arrests, but it lacks clear safeguards, judicial oversight, and accountability measures. This created risks of abuse and weakens public trust. In contrast, other countries require judicial warrants, have clear appeal systems, and provide independent oversight to ensure fairness and respect for privacy. The study also noted challenges in Zambia such as limited resources, low public awareness, and unclear procedures for handling seized property. Lessons from the United Kingdom, South Africa, Kenya, and Nigeria show that strong enforcement can coexist with respect for human rights when supported by transparency and accountability. The study recommends judicial oversight, independent monitoring, clear guidelines for inspectors, and proper procedures for seized property to strengthen Zambia's data protection enforcement and promote public confidence in digital governance.

CHAPTER ONE

1.0 INTRODUCTION

In today's digital world, personal information is shared and stored online more than ever before. This includes names, addresses, phone numbers, and even financial details. While this makes life more convenient, it also brings risks. If this information is not protected properly, it can be misused or stolen. To address this, many countries have created laws to protect people's personal data.

Zambia introduced the Data Protection Act in 2021. This law aims to ensure that personal data is handled safely and responsibly. It sets rules for how organizations collect, use, and store personal information. It also gives certain powers to inspectors to check if organizations are following the law. These powers include entering offices, checking records, and even making arrests.[1]

However, there are concerns about how these powers are used. Some people worry that inspectors have too much authority without enough oversight. There are also questions about what happens to property that is taken during inspections. Without clear rules, there's a risk that people's rights could be violated.[2]

This thesis will look at how Zambia's data protection enforcement compares to similar laws in South Africa, Kenya, Nigeria, and the United Kingdom. The goal is to understand how these countries balance the need to enforce data protection laws with the need to protect individual rights.

1.1 BACKGROUND OF THE STUDY

The protection of personal data is a growing concern worldwide. As more services move online, the amount of personal information being collected increases. This has led to the creation of data protection laws in many countries. These laws are designed to ensure that personal information is handled securely and that individuals' privacy is respected.[3]

In Zambia, the Data Protection Act was enacted in 2021. This law established the Data Protection Commission, which is responsible for overseeing data protection practices in

[1] Act 3 of 2021

[2] https://www.dataprotection.gov.zm (Accessed on 20/04/2025)

[3] https://www.nadpa-rapdp.org/en/node/220 (Accessed on 20/04/2025)

the country. The Commission's duties include registering data controllers and processors, licensing data auditors, and ensuring compliance with the law. Starting in March 2025, the Commission began actively enforcing the Act, requiring organizations to register and adhere to data protection standards.[4]

Despite these efforts, there are challenges in enforcing the Data Protection Act effectively. One major issue is the lack of public awareness about data protection rights. Many individuals are unaware of how their personal information should be handled or what their rights are under the law. This lack of knowledge can lead to underreporting of data breaches and limited accountability for organizations that mishandle data.[5]

Another significant challenge is the limited resources available to the Data Protection Commission. Insufficient funding and staffing can hinder the Commission's ability to monitor compliance, investigate complaints, and enforce penalties for violations. This can result in delays in addressing data protection issues and erode public trust in the enforcement system.[6]

Furthermore, the law grants inspectors broad powers to enforce data protection regulations. These powers include entering business premises, inspecting records, and making arrests without a warrant. However, there are concerns about the lack of clear guidelines and oversight mechanisms to prevent the abuse of these powers. For example, the procedures for handling seized property are not well-defined, which can lead to prolonged detention of property and affect individuals' rights.

These enforcement challenges highlight the need to examine how Zambia's data protection enforcement compares to that of other countries. By analyzing the enforcement-related provisions in the data protection laws of South Africa, Kenya, Nigeria, and the United Kingdom, this study aims to identify best practices and recommend improvements to Zambia's enforcement framework.

1.2 STATEMENT OF THE PROBLEM

The current legal framework governing data protection in Zambia provides a robust framework for personal data processing, emphasizing the roles of data controllers,

[4] https://www.nadpa-rapdp.org/en/node/220 (Accessed on 20/04/2025)
[5] Understanding Data Protection and Privacy Laws in Zambia https://generisonline.com/understanding-data-protection-and-privacy-laws-in-zambia (Accessed on 20/04/2025)
[6] Ibid

processors, and the enforcement powers of inspectors. However, significant gaps exist in the practical enforcement of these laws, particularly concerning the authority and operational effectiveness of inspectors. **Sections 7 to 10 of the Data Protection Act**[7]confer broad powers to inspectors, including the authority to enter business premises, audit records, remove documents, and make arrests without warrants. Despite these powers, there is no clear and enforceable mechanism ensuring the inspectors' accountability or guidelines to prevent the abuse of these powers.

For instance, **Section 8** [8]allows inspectors to remove documents or other items without sufficient safeguards, and **Section 9** [9]grants them the power to make arrests without a warrant. However, the law lacks clear procedures on how inspectors are monitored or held accountable for the exercise of these invasive powers. This creates room for potential misuse, especially in cases where the boundaries between lawful enforcement and abuse of authority could be blurred. Furthermore, while **Section 11** [10]mandates the restoration of seized property, the process for handling disputed property or goods remains unclear, especially when the enforcement officer is satisfied that the person cannot be found. The ambiguity in these provisions may lead to prolonged detention of property or delays in the return of items that have been wrongfully seized, affecting individuals' property rights and businesses' operations.

The lack of clear oversight mechanisms and comprehensive procedures for enforcement has led to a lack of public trust in the inspectorate’s ability to uphold the law impartially. This loophole undermines the effectiveness of Zambia’s data protection laws and raises concerns about the protection of individuals' rights and privacy.

The problem, therefore, lies in the absence of specific measures to address the accountability of inspectors, the clarity in the procedures for handling seized property, and the potential for the abuse of powers granted under the law. These gaps hinder the overall success of data protection efforts, and this thesis aims to highlight these issues and propose actionable recommendations for strengthening the enforcement framework.

[7] Data Protection Act No. 3 of 2021
[8] Data Protection Act No. 3 of 2021
[9] Ibid
[10] Data Protection Act No. 3 of 2021

1.3 RESEARCH OBJECTIVES

1. To explore the concepts of Cyber Scurity and Cyberc crimes.
2. To explore the legal framework governing Cyber Security and Cyber Crimes in Zambia.
3. To compare human rights safeguards in enforcement- related provisions of the Zambian Data Protection Act with those in counterpart legislation in Nigeria, South Africa, Kenya, and the United Kingdom.

1.4 RESEARCH QUESTIONS

1. What are the concepts of Cyber Security and Cyber Crimes?
2. What is the legal framework governing Cyber Security and Cyber Crimes in Zambia?
3. How do human rights safeguards in the enforcement-related provisions of the Zambian Data Protection Act compare with those in counterpart legislation in Nigeria, South Africa, Kenya, and the United Kingdom?

1.5 SIGNIFICANCE OF THE STUDY

This study is important because it focuses on how to make sure that the powers given to inspectors under Zambia's Data Protection Act are used fairly and responsibly. It aims to help improve public trust in data protection by suggesting clear rules and safeguards that prevent abuse of power. The findings will also help lawmakers, the Data Protection Commission, businesses, and the public understand where the current enforcement system is weak and what can be done to strengthen it. By comparing Zambia with countries like South Africa, Kenya, Nigeria, and the UK, the study offers practical lessons that can guide reforms and improve the way data protection is enforced in Zambia.

1.6 SCOPE OF THE STUDY

This study focuses only on the enforcement part of Zambia's data protection laws, especially the roles and powers of inspectors. It does not cover all areas of data protection, such as consent, data transfer, or data subject rights. The study looks at the possible risks of misuse of inspector powers like warrantless arrests and property seizures. It also includes a comparison with similar enforcement systems in South Africa, Kenya, Nigeria, and the United Kingdom to help draw useful lessons for Zambia. The study uses both legal analysis and real-world examples to support its findings.

1.7 LITERATURE REVIEW

Alex B. Makulilo[11] discusses how African countries, including Zambia, have embraced technology to build their economies. He notes that the rapid growth of mobile phone use and internet access has transformed how people communicate and do business. However, this digital growth also brings challenges in protecting personal information. While Makulilo highlights the importance of technology in Africa's development, this study focuses on how Zambia's data protection laws are enforced, especially the role of inspectors in safeguarding personal data.

Justin Bryant[12] emphasizes that data protection laws should address the unique risks faced by young people, who are the most active users of digital technologies. He suggests that lawmakers need to understand the technologies popular among youth and the potential data protection issues they present. While Bryant focuses on youth and their interaction with technology, this study examines the broader enforcement mechanisms of data protection laws in Zambia, including how inspectors' powers are regulated to prevent misuse.

Kholofelo Kugler[13] explores the impact of data protection laws on international trade and investment. He argues that inadequate data protection can deter foreign businesses from operating in a country. While Kugler's work centers on the economic implications of data protection, this study delves into the enforcement aspects within Zambia, assessing whether current laws and inspector powers effectively protect personal data and support economic growth.

Sam Phiri[14] analyzes the balance between the right to information and the right to privacy in Zambia. He stresses the need for laws that protect personal data in the digital age. While Phiri focuses on the legal rights of individuals, this study investigates how these

[11] African Data Privacy, (Springer International Publishing AG) 2016
[12] Justin Bryant. Africa in the Information Age: Challenges, Opportunities and Strategies for Data Protection and Digital Rights. Stan Tech. 2021
[13] Kholofelo Kugler. The Impact of Data Localisation Laws on Trade in Africa. Mandela Institute. 2022
[14] Sam Phiri. Zambia Digital Rights Landscape Report. Digital Rights in Closing Civic Space: Lessons from Ten African Countries. 2021

rights are upheld in practice, particularly through the actions and oversight of data protection inspectors.

Michael Pisa, Pam Dixon, and Ugonma Nwankwo[15] highlight the importance of robust data protection laws and the need for regular reviews to ensure they remain effective. They advocate for clear accountability mechanisms within these laws. While their work emphasizes the legislative framework, this study concentrates on the practical enforcement of these laws in Zambia, focusing on how inspectors' powers are exercised and monitored to protect individuals' personal data.

Greenleaf [16]wrote widely about the development of data protection laws in Africa. He explained that many African countries have passed data protection laws, but very few actually enforce them. He said the problem is not the law itself but the lack of action in applying the law. He pointed out that the people responsible for enforcing the law often lack training, resources, and clear rules to follow. This study goes further by focusing specifically on inspectors in Zambia. It looks at the wide powers they have, how those powers could be misused, and the absence of accountability. Greenleaf mainly looked at the gap between law and practice, but this study goes deeper into how the enforcement powers themselves may be a problem.

Reventlow [17]focused on the risks that come with giving state agents powers to access, collect, or seize personal data without checks and balances. She said this creates room for abuse and can make people afraid to share their information, even when it's needed for development. She stressed that without clear limits and oversight, even well-meaning laws can hurt people’s rights. Reventlow talked generally about state overreach and privacy rights. This study focuses more specifically on Zambia’s inspectors and how they operate under the Data Protection Act. It highlights the danger of warrantless arrests and unclear procedures around seized property, which Reventlow did not address in detail.

[15] Michael Pisa , Pam Dixon, and Ugonma Nwankwo. Why Data Protection Matters for Development: The Case for Strengthening Inclusion and Regulatory Capacity. Center for Global Development. 2021

[16] Greenleaf, G. (2018). Global Data Privacy Laws 2017: 120 National Data Privacy Laws, Including African Developments.

[17] Reventlow, N. J. (2021). Protecting Privacy in the Age of Surveillance. Digital Freedom Fund.

Dr. Powell [18]studied data protection in the UK and noted that inspectors, known there as ICO officers, have strict rules to follow when entering business premises. She emphasized that even in developed countries, enforcement must be balanced with strong accountability. She warned that when people do not trust those enforcing the law, the entire system becomes weak. While Powell looked at the UK, this study looks at Zambia, where the enforcement environment is very different. UK inspectors work under clear, public rules, while Zambian inspectors have broad powers but little oversight. This study shows how this gap can lead to abuse or delays in returning wrongly seized property.

Kapiyo[19] looked at data protection enforcement in Kenya. He pointed out that despite having laws and a data commissioner, enforcement was still poor because the commissioner had no strong team of inspectors. He said most enforcement actions were delayed or never happened, and public awareness was also low, making it easier for violations to go unpunished. Kapiyo focused on lack of enforcement and public knowledge. This study focuses on the other side what happens when enforcement does occur, but without clear procedures. It deals with real risks that can come from giving inspectors too much power without proper checks.

B. Kamleitner and V. Mitchell [20]focus on the concept of interdependent privacy in their study. They argue that personal data shared by individuals can extend to third parties, often without their consent. Their example illustrates how a smartphone app, when downloaded, can access not just the user's personal data but also the contacts in their phone, sharing this third-party data without their permission. This situation creates privacy risks, as individuals unknowingly become the gatekeepers of others' private information. Their work highlights the challenges of managing data sharing, especially in digital environments, which is crucial for understanding the risks in Zambia's data protection system. However, this study differs by focusing specifically on how Zambia's data protection framework can address the accountability and oversight of data inspectors,

[18] Powell, A. (2020). Data Trust and Accountability in the UK's Information Commissioner's Office. London School of Economics.

[19] Kapiyo, V. (2019). Challenges in Implementing Data Protection Laws in Kenya. CIPESA Reports.

[20] B. Kamleitner and V. Mitchell, Your Data Is My Data: A Framework for Addressing Interdependent Privacy Infringements/ 25th July, 2019 Vol 38 Journal of Public Policy and Marketing

ensuring that the misuse of data-sharing powers, like those illustrated by Kamleitner and Mitchell, is minimized.

Youngson M. Ndawana's[21]research examines internet freedom in Zambia, emphasizing the importance of laws that allow citizens to express themselves freely online and access information. Ndawana argues that these freedoms are vital for a modern society but does not focus on the potential risks, such as the protection of personal data when shared across borders. The study overlooks how internet freedoms might conflict with data protection laws, particularly regarding cross-border data movement. In contrast, this study addresses those very concerns, exploring how Zambia's data protection laws can better safeguard personal data and prevent misuse in cross-border contexts. This research builds on Ndawana's ideas but delves deeper into the gaps in enforcement, especially regarding the role and accountability of inspectors.

1.8 METHODOLOGY

This study uses a **qualitative research approach** to understand how the Data Protection Act is being enforced in Zambia and to look at the powers given to inspectors. Qualitative research is the best method for this study because it helps us understand people's real experiences, thoughts, and views. It gives deeper information that numbers or statistics alone cannot provide. This is important when looking at how inspectors are using their powers and whether the law is working as it should.

The study will focus on collecting information from people who are directly involved or affected by the enforcement of the Data Protection Act. This includes officers from the Data Protection Commission, legal experts, civil society groups, and people who may have experienced inspections or enforcement actions. Their views will help us understand how the law is working in real life and what problems exist.

1.8.1 Data Collection

[21] Youngson M. Ndawana. State of the internet Freedom in Zambia. Liverpool John Moores University. 2017

Information will be collected through **interviews** and **document analysis**. The interviews will be done with people who are familiar with how the data protection law is enforced. This includes staff from the Data Protection Commission, officials from the Ministry of Technology and Science, and people from civil society groups that work on human rights and data protection. These interviews will help us understand how inspectors carry out their work, what challenges they face, and whether people feel protected under the current system.

The study will also review **existing documents** such as official reports, media articles, research papers, and documents from civil society and human rights organizations. These documents will provide background information and show what is happening on the ground in terms of enforcement, accountability, and the use of inspectors' powers.

1.8.2 Data Analysis

The information collected from interviews and documents will be examined using **thematic analysis**. This means we will look for common topics, patterns, or issues that appear again and again in the responses and documents. For example, if many people talk about fear of abuse of power by inspectors, that will be a theme. If others talk about lack of training or unclear rules, those will also be noted.

The goal is to clearly show what is working and what is not, and to point out the main problems that need attention. Thematic analysis makes it easier to organize and explain the key findings in a simple and clear way.

1.8.3 Limitations

One challenge in this study is that it may not be possible to interview everyone involved in the enforcement of data protection laws. The number of people interviewed will be limited. However, the study will try to include a variety of people from both government and non-government sectors so that we can get different views and make sure the findings are balanced and helpful.

1.9 ETHICAL CONSIDERATIONS

The researcher will make sure to obtain correspondence introducing her outlining that information collected is for academic purposes from the beginning in order to uphold high moral and ethical standards. The researcher promises to keep the data they collect secret and to use it only for academic study. Furthermore, the researcher shall credit the works of other authors in order to protect their copyright and free usage while using the OSCOLA referencing style.

CHAPTER TWO

THE CONCEPTS OF CYBER SCURITY AND CYBERC CRIMES

2.0 INTRODUCTION

This chapter was based on examining the concepts of cybersecurity and cybercrime, focusing on how digital systems are protected and the legal frameworks in place to combat crimes committed using technology. Cybersecurity is about keeping computers, networks, and data safe from harm, using tools like antivirus software, firewalls, and encryption, as well as following best practices to prevent threats such as hacking, phishing, and ransomware. Cybercrime occurs when someone uses digital systems to commit illegal acts, from stealing personal information to disrupting critical services. The chapter also looks at international instruments designed to fight cybercrime, such as the United Nations Convention Against Cybercrime and the African Union's Malabo Convention, which provide guidelines for national policies, legal measures, and international cooperation. These instruments emphasize the importance of protecting citizens' rights, securing critical infrastructure, promoting a culture of cybersecurity, and establishing effective institutions and sanctions to address cybercrime while ensuring collaboration across borders.

2.1 WHAT IS CYBERSECURITY?

Cybersecurity is all about keeping our computers, phones, networks, and data safe from harm. It involves using tools like antivirus software, firewalls, and encryption, along with following rules and best practices to prevent threats such as viruses, hackers, phishing scams, and ransomware.[22] Cybersecurity is also known as information security or system security, and its goal is to protect our digital lives and make sure our devices and information stay private and secure.[23][24]

Every day, we depend on digital systems for almost everything we do. From checking our bank account and texting friends, to shopping online or using government services, these

[22] GeeksforGeeks "What is Cyber Security?", explaining the tools and purpose of cybersecurity https://www.geeksforgeeks.org/ethical-hacking/what-is-cyber-security

[23] IBM "What is cybersecurity?" offering clear definitions of systems, people, and data protection. https://www.ibm.com/think/topics/cybersecurity

[24] ScienceNewsToday "Cybersecurity Is a Human Right" describing our digital skeleton and dignity

systems help us live our lives.[25] If cybersecurity fails, our personal information like passwords or financial details can get stolen. That can lead to identity theft, money loss, and a broken trust in the systems we use. Cybersecurity plays the same comforting role online that a lock and alarm do for our homes.[26]

In a very real sense, cybersecurity matters not just because of the tools it matters because of what's at stake. Cyberattacks can cost billions or even trillions of dollars worldwide. One study projects that cybercrime could cost the world economy $10.5 trillion in 2025.[27] With cyber threats on the rise and getting more sophisticated like attacks powered by artificial intelligence the risks are rising fast.[28]

More than just big numbers, the real danger is that our lives are woven into digital systems. Our photos, private messages, health details, and banking history form a "digital skeleton" of our lives in the cloud and on servers. Losing control of that data is like having intruders tamper with personal parts of our lives. Cybersecurity helps keep that digital skeleton intact, protecting both our privacy and our dignity.[29]

When it comes to why cybersecurity truly matters, think about this: for individuals, it safeguards private information and finances. For businesses, it protects their operations, reputation, and keeps customer data secure. For governments, it defends critical systems like healthcare, power grids, and transportation. Cybersecurity is a shared need, from the smallest smartphone to the biggest institution.[30]

Cybersecurity does more than stop attacks it ensures that our digital tools work when we need them. It maintains the confidentiality of our data (so only the right people see it), ensures integrity (so data isn't altered unknowingly), and keeps services available. For instance, encryption scrambles messages so only the rightful person can read them.[31] A

---

[25] Ibid

[26] https://dsisecurity.com/2021/08/09/the-importance-of-cybersecurity-in-todays-society (Accessed on 14/08/2025)

[27] IBM "What is cybersecurity?" offering clear definitions of systems, people, and data protection. https://www.ibm.com/think/topics/cybersecurity

[28] IBM "What is cybersecurity?" offering clear definitions of systems, people, and data protection. https://www.ibm.com/think/topics/cybersecurity

[29] ScienceNewsToday "Cybersecurity Is a Human Right" describing our digital skeleton and dignity Cybersecurity Explained: The Basics of Protecting Your Digital Life

[30] Ibid

[31] Kemper, Grayson (2019-08-01). "Improving employees' cyber security awareness". *Computer Fraud & Security*. **2019**

locked HTTPS website, email encryption, or a VPN makes it much harder for attackers to intercept or misuse data.[32]

But cybersecurity isn't just about technology it also depends on people. The human element is often the weakest link. Cybercriminals exploit social engineering, phishing, and scareware to trick people into giving up info or downloading harmful files. Being aware of these tricks, using strong and unique passwords, and turning on two-factor authentication are key ways we protect ourselves.[33]

2.2 WHAT IS CYBERCRIME?

Cybercrime happens when someone uses computers, phones, or the internet to do something illegal. It can be as simple as tricking someone out of money or as complex as hacking into a government system. Criminals might break into accounts, steal private information like social security numbers or credit card details, or spread lies to trick people.[34] They might also share harmful material, such as malware or private content, without permission. These acts cause harm by taking money, ruining reputations, and violating privacy. Cybercriminals often exploit the trust and convenience we place in digital devices to commit crimes that would be much harder in the physical world. According to Sukhai, Nataliya B,[35] cybercrime covers a wide range of actions using digital devices or networks, from hacking and data theft to disrupting services or damaging reputations.

When a crime could not happen without computers, that is called cyber-dependent crime. Think of malware that locks your files unless you pay a ransom, or a denial-of-service attack that floods a website with traffic to knock it offline, or a hacker who breaks into a system to steal data. These crimes depend entirely on digital systems to exist. United Nations University defines these crimes as ones that rely on computers or networks

[32] GeeksforGeeks "What is Cyber Security?", explaining the tools and purpose of cybersecurity https://www.geeksforgeeks.org/ethical-hacking/what-is-cyber-security

[33] Kim, Lee (April 2017). "Cybersecurity awareness: Protecting data and patients". Nursing Management.

[34] Freeze, Di (12 October 2023). "Cybercrime To Cost The World $9.5 trillion USD annually in 2024". *Cybercrime Magazine*.

[35] Sukhai, Nataliya B. (8 October 2004). "Hacking and cybercrime". *Proceedings of the 1st annual conference on Information security curriculum development*. New York, NY, USA: ACM

themselves. Researchers say they threaten the core of digital systems by compromising integrity, availability, or confidentiality of data.[36]

2.2.1 Why cybercrime keeps growing at such a fast pace

Cybercrime is rising because technology makes it easy, fast, and often anonymous to commit crimes across borders. Criminals can hide behind VPNs or encrypted networks, making it very difficult for police to trace them. This anonymity emboldens criminals to act more often and more boldly. Security experts explain that tools such as Tor, VPNs, and encrypted messaging disguise identity, making it harder for law enforcement to catch the wrongdoers.[37] The internet also connects people, businesses, and governments across the world, so attackers can target victims far away without ever being detected.[38]

Digital systems are everywhere now in homes, workplaces, hospitals, and even in IoT devices like smart fridges or voice assistants. Because more parts of daily life are digital, there are more opportunities for criminals to exploit. Devices with weak security or outdated software are easy targets. The growing digitization of everything increases what experts call the “attack surface” more chances and entry points for cybercriminals.[39]

Cybercrime is also attractive to criminals because it often yields a big payoff for relatively little effort. Small businesses, for example, may lack strong security but store valuable customer or financial data, making them prime targets. Cybercriminals know this and take advantage.[40] Cryptocurrency adds another layer of appeal by allowing criminals to receive payment without easily being traced. Tools like mixers make laundering these funds easier than ever.[41]

No surprise then that the financial damage from cybercrime is enormous and growing. Cyber Defense Magazine reports that by the end of 2025, global costs from cybercrime could reach between $1.2 trillion and $1.5 trillion annually. This includes direct financial

---

[36] Global Initiative Against Transnational Organized Crime. Definition of cyber-dependent & impact on data. https://globalinitiative.net/wp-content/uploads/2019/03/TGIATOC-Report-Cybercrime-in-the-UN-01Mar1510-Web.pdf

[37] Wipul Jayawickrama, Cyber Crime—Threats, Trends and Challenges, Computer Security Week 2008, Info Shield, 2008

[38] "Guillaume Lovet Fortinet, Fighting Cybercrime: Technical, Juridical and Ethical ChallengesVIRUS BULLETIN CONFERENCE, 2009"

[39] Security Law blog. Anonymity, IoT, and cybercrime growth factors. https://www.security.law/post/cybercrime-growth-is-unstoppable-and-these-are-the-reasons-why

[40] Ibid

[41] Ibid

losses, downtime, brand damage, nation-state attacks, and cyber insurance costs.[42] Earlier estimates are even higher Cybersecurity Ventures projects that by 2025, cybercrime damages could reach $10.5 trillion a year, up from $3 trillion in 2015.[43] Interpol warns that the value lost each year is now comparable to the GDP of major countries, highlighting the global economic impact of cybercrime.[44]

Beyond money, cybercrime undermines trust in systems we depend on. People lose confidence in online banking or voting when these systems are compromised. Businesses suffer reputational harm, which may cost more than the actual breach. Hospitals may be forced to postpone surgeries; entire supply chains can face disruption. These ripple effects can affect communities and even national security.[45]

2.3 INTERNATIONAL INSTRUMENTS TO FIGHT CYBERCRIME

To tackle cybercrime and enhance cybersecurity, the world has created several international instruments treaties, conventions, and regional agreements.

2.4 UNITED NATIONS CONVENTION AGAINST CYBERCRIME

The United Nations Convention Against Cybercrime, adopted on December 24, 2024, represents a significant milestone in the global effort to combat cybercrime. This treaty aims to establish a comprehensive international legal framework to address the increasing threats posed by cybercriminal activities. The Convention's adoption followed extensive negotiations and reflects the UN's commitment to enhancing international cooperation in the fight against cybercrime.[46]

2.4.1 Purpose and Objectives

The primary objectives of the Convention are to promote and strengthen measures to prevent and combat cybercrime more efficiently and effectively, facilitate international cooperation in preventing and combating cybercrime, and support technical assistance

---

[42] https://www.cyberdefensemagazine.com/the-true-cost-of-cybercrime-why-global-damages-could-reach-1-2-1-5-trillion-by-end-of-year-2025 (Accessed on 14/08/2025)

[43] https://www.bdemerson.com/article/complete-cybercrime-statistics? (Accessed on 14/08/2025)

[44] INTERPOL. Economic impact of cybercrime. https://www.interpol.int/en/Crimes/Cybercrime? (Accessed on 14/08/2025)

[45] Investopedia and NumberAnalytics. Business, reputational and societal impact of cybercrime. https://www.investopedia.com/financial-edge/0112/3-ways-cyber-crime-impacts-business.aspx (Accessed on 14/08/2025)

[46] United Nations Office on Drugs and Crime (UNODC). (2024). *United Nations Convention against Cybercrime*. Retrieved from https://www.unodc.org/unodc/en/cybercrime/convention/home.html

and capacity-building, particularly for developing countries. These objectives are outlined in Article 1 of the Convention, emphasizing the need for a coordinated global response to cyber threats.

2.4.2 Purpose and Scope

The primary objectives of the Convention are to promote and strengthen measures to prevent and combat cybercrime more efficiently and effectively, facilitate international cooperation in preventing and combating cybercrime, and support technical assistance and capacity-building, particularly for developing countries.

The scope of the Convention is outlined in **Article 3**[47], which specifies that it applies to the prevention, investigation, and prosecution of criminal offenses established in accordance with the Convention. This includes the freezing, seizure, confiscation, and return of proceeds from such offenses, as well as the collection, obtaining, preservation, and sharing of electronic evidence for the purpose of criminal investigations or proceedings.

2.4.3 Human Rights Considerations

A critical aspect of the Convention is its emphasis on human rights. **Article 6** [48]mandates that States Parties ensure the implementation of their obligations under the Convention is consistent with international human rights law. Furthermore, it explicitly states that nothing in the Convention shall be interpreted as permitting the suppression of human rights or fundamental freedoms, including freedoms of expression, conscience, opinion, religion or belief, peaceful assembly, and association. These provisions aim to safeguard individual rights while combating cybercrime.

2.4.4 Criminal Offenses Defined

The Convention delineates various cybercrime offenses that States Parties are required to criminalize under their domestic laws. **Article 7** [49]addresses illegal access to ICT systems, making it an offense to intentionally access any part of an ICT system without authorization. **Article 8** [50]focuses on illegal interception, criminalizing the unauthorized

[47] United Nations Office on Drugs and Crime (UNODC). (2024). *United Nations Convention against Cybercrime*. Retrieved from https://www.unodc.org/unodc/en/cybercrime/convention/home.html
[48] Ibid
[49] Ibid
[50] United Nations Office on Drugs and Crime (UNODC). (2024). *United Nations Convention against Cybercrime*. Retrieved from https://www.unodc.org/unodc/en/cybercrime/convention/home.html

interception of non-public transmissions of electronic data. Article 9 pertains to interference with electronic data, prohibiting actions that damage, delete, deteriorate, alter, or suppress electronic data without right. **Article 10** [51]targets interference with ICT systems, criminalizing acts that seriously hinder the functioning of an ICT system by manipulating electronic data. **Article 11** [52]addresses the misuse of devices, making it an offense to obtain, produce, sell, or possess devices or data intended for committing cybercrime offenses. Article 12 concerns ICT system-related forgery, criminalizing the input, alteration, deletion, or suppression of electronic data resulting in inauthentic data. **Article 13** [53]deals with ICT system-related theft or fraud, criminalizing actions that cause a loss of property through deception or interference with ICT systems. These articles collectively establish a comprehensive legal framework for addressing various forms of cybercrime.

2.4.5 International Cooperation and Jurisdiction

The Convention emphasizes the importance of international cooperation in combating cybercrime. **Article 22** [54]outlines the jurisdictional scope of the treaty, specifying that each State Party shall establish jurisdiction over offenses committed within its territory or on board a vessel or aircraft registered under its laws. It also allows for jurisdiction over offenses committed against nationals or by nationals of the State Party, even if the offense occurs outside its territory. This provision ensures that States Parties can effectively prosecute cybercrimes with international dimensions.

2.4.6 AFRICAN UNION'S MALABO CONVENTION

The African Union Convention on Cyber Security and Personal Data Protection, also known as the Malabo Convention, is a significant legal framework adopted on June 27, 2014, during the 23rd Ordinary Session of the African Union Summit in Malabo, Equatorial Guinea. This Convention aims to establish a comprehensive legal structure to enhance cybersecurity, regulate electronic transactions, and protect personal data across the African continent. It serves as a response to the increasing reliance on information and

[51] Ibid
[52] Ibid
[53] Ibid
[54] Ibid

communication technologies (ICTs) and the associated risks of cyber threats and data breaches.[55]

The Convention is structured into several parts, each addressing different aspects of cybersecurity and data protection. Part III, titled "Promoting Cyber Security and Combating Cyber Crime," focuses on measures to be taken at the national level to strengthen cybersecurity frameworks. Section I of this part outlines the obligations of State Parties to develop national cybersecurity policies and strategies. Article 24 emphasizes the importance of creating a national cybersecurity framework that includes a policy recognizing the significance of Critical Information Infrastructure (CII) and identifying risks using an all-hazards approach. It also mandates the adoption of strategies to implement the policy, covering areas such as legislative reform, sensitization, capacity-building, public-private partnerships, and international cooperation.

Article 25 addresses legal measures against cybercrime. It requires State Parties to adopt legislative and regulatory measures to criminalize acts affecting the confidentiality, integrity, availability, and survival of ICT systems and data. Additionally, it mandates the establishment of national regulatory authorities with specific responsibilities in cybersecurity, including response to incidents, coordination, and cooperation in forensic investigations and prosecution. Importantly, these measures must respect the rights of citizens as guaranteed under national constitutions and international human rights instruments, ensuring that actions taken do not infringe upon freedoms such as expression, privacy, and the right to a fair hearing.

Article 26 [56]focuses on promoting a culture of cybersecurity. It calls for the development of a cybersecurity culture among all stakeholders, including governments, enterprises, and civil society. State Parties are encouraged to establish cybersecurity plans for government systems, implement sensitization programs for users, and foster involvement from the private sector and civil society. Education and training are also emphasized, with measures to develop capacity-building initiatives and set standards for the private sector.

[55] African Union. (2014). *African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention)*. Malabo, Equatorial Guinea. Retrieved from https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

[56] Ibid

Article 27 [57]outlines the establishment of national cybersecurity monitoring structures. It requires State Parties to adopt measures to establish appropriate institutional mechanisms responsible for cybersecurity governance. These measures should establish clear accountability at all levels of government, express a public commitment to cybersecurity, and encourage private sector participation. Additionally, an institutional framework should be established to combat cybercrime, ensure monitoring and response to incidents, and facilitate national and cross-border coordination.

Article 28 emphasizes the importance of international cooperation. It encourages State Parties to harmonize legislative measures to strengthen regional cooperation and respect the principle of double criminal liability. Mutual legal assistance agreements should be encouraged, and the exchange of information on cyber threats and vulnerabilities should be promoted. State Parties are also urged to utilize existing means for international cooperation, including international, intergovernmental, regional, and public-private partnerships.

Section II of Part III addresses criminal provisions related to information and communication technologies. Article 29 outlines offenses specific to ICTs, including unauthorized access to computer systems, fraudulent data entry, and hindering or distorting the functioning of computer systems. It also criminalizes the unlawful production, sale, or possession of devices or data designed to commit offenses. State Parties are required to adopt regulations compelling vendors to assess the security of their products and disclose vulnerabilities to consumers.

Article 30 [58]focuses on adapting certain offenses to ICTs. It mandates the criminalization of property offenses such as theft, fraud, and blackmail involving computer data. The use of ICTs to commit offenses is considered an aggravating circumstance. Additionally, the violation of protected systems, particularly those related to national defense, is to be criminalized. Criminal liability for legal persons is also established, holding organizations accountable for offenses committed on their behalf.

---

[57] African Union. (2014). *African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention)*. Malabo, Equatorial Guinea. Retrieved from https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

[58] African Union. (2014). *African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention)*. Malabo, Equatorial Guinea. Retrieved from https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

Article 31 [59]addresses the adaptation of sanctions to ICTs. It requires State Parties to ensure that offenses under the Convention are punishable by effective, proportionate, and dissuasive criminal penalties. Legal persons found liable are subject to sanctions, including criminal fines. Additional sanctions may be imposed for offenses committed through digital communication mediums, and breaches of data confidentiality are to be penalized similarly to breaches of professional secrecy.

The Convention also outlines procedural law measures. State Parties are required to adopt legislative measures to ensure that data stored in computer systems can be accessed during investigations. Judicial authorities may carry out searches and seize data as necessary. Preservation orders may be imposed to protect data integrity during investigations, and appropriate technical means may be used to collect or record data in real-time.

2.5 CONCLUSION

This chapter has shown that cybersecurity and cybercrime are deeply connected to how modern societies use digital technology. Effective cybersecurity requires not just technical tools but also legal frameworks, education, and collaboration between governments, businesses, and civil society. The United Nations Convention Against Cybercrime and the African Union Malabo Convention provide clear guidance on developing national policies, criminalizing cyber offenses, and fostering international cooperation. They emphasize respecting human rights, protecting critical infrastructure, and creating a culture of security among all users. By following these conventions, states can better prevent cybercrime, respond to incidents, and ensure that digital systems remain safe, trustworthy, and functional for individuals, businesses, and governments alike.

[59] Ibid

CHAPTER THREE

THE LEGAL FRAMEWORK GOVERNING CYBER SECURITY AND CYBER CRIMES IN ZAMBIA

3.0 INTRODUCTION

Chapter Three examines the legal framework governing cyber security and cyber crimes in Zambia, focusing on how the law protects information systems, critical infrastructure, and individuals from digital threats. With the growth of online services, digital transactions, and the use of computers across all sectors, Zambia has developed specific legislation, including the Data Protection Act No. 3 of 2021, the Cyber Security Act No. 3 of 2025, and the Cyber Crimes Act No. 4 of 2025, to regulate the use, protection, and enforcement of data and information systems. These laws establish institutions, set out offences, and define penalties to ensure accountability, prevent abuse, and safeguard personal and national data. While the framework provides strong powers to inspectors and agencies, such as entering premises, seizing property, and investigating cyber threats, practical enforcement faces challenges, including potential abuse of powers, unclear procedures for restoring seized property, and the need for oversight mechanisms. This chapter highlights the strengths and limitations of these laws, showing how they aim to balance effective enforcement with the protection of rights and the promotion of trust in Zambia's digital environment.

3.1 THE DATA PROTECTION ACT NO. 3 OF 2021

The **Data Protection Act**[60] provides for the establishment of an inspectorate to oversee compliance with data protection laws in Zambia. According to **Section 7(1),**[61] the Civil Service Commission may appoint a suitably qualified person to serve as an inspector for the purposes of ensuring compliance with the Act. The appointed inspector is issued with an identification card and a certificate of appointment, which serve as prima facie evidence of their authority, as provided under **Section 7(2).**[62]These measures are intended to ensure that only competent and officially recognized individuals can exercise

[60] Act No. 3 of 2021
[61] Ibid
[62] Ibid

inspection powers, which include monitoring the processing of personal data and investigating possible breaches by data controllers and processors.

Inspectors play a vital role in the protection of personal data. Their duties involve reviewing records, auditing practices, and ensuring that organizations follow the rules on how personal information is collected, stored, and shared. They also have the responsibility of protecting the rights of data subjects, who are individuals whose information is being processed. By carrying out inspections and investigations, inspectors help prevent misuse or unlawful disclosure of personal data, which is essential in a country where online transactions and digital data collection are becoming increasingly common.[63]

Despite these important functions, the Act does not provide detailed guidance on the accountability of inspectors. There are no clear mechanisms to monitor their actions or to prevent abuse of power. This lack of oversight creates a risk that inspectors could act arbitrarily or go beyond their legal authority, which could lead to violations of privacy and property rights. The absence of procedures to review inspectors' conduct may also reduce public confidence in the enforcement of data protection laws, as individuals and businesses may fear unfair treatment during inspections.[64]

Section 7[65] establishes the foundation for the inspectorate, but for it to be effective, additional measures are needed to ensure transparency and accountability. This could include internal reporting systems, regular audits of inspectors' actions, and clear procedures for handling complaints against them. Without such safeguards, the powers granted under the Act, though necessary for enforcement, may not be exercised in a fair and consistent manner, limiting the overall effectiveness of Zambia's data protection framework. Ensuring accountability is therefore critical to maintaining trust and compliance in the rapidly growing digital environment.[66]

---

[63] Understanding Data Protection and Privacy Laws in Zambia https://generisonline.com/understanding-data-protection-and-privacy-laws-in-zambia (Accessed on 20/04/2025)

[64] Justin Bryant. Africa in the Information Age: Challenges, Opportunities and Strategies for Data Protection and Digital Rights. Stan Tech. 2021

[65] Act No. 3 of 2021

[66] Understanding Data Protection and Privacy Laws in Zambia https://generisonline.com/understanding-data-protection-and-privacy-laws-in-zambia (Accessed on 20/04/2025)

3.2 POWERS OF INSPECTORS AND LIMITATIONS

Section 8 of the Data Protection Act[67] clearly sets out the powers of inspectors in Zambia. Inspectors are authorized to enter the business premises of data controllers or processors, inspect equipment and supplies, examine documents, make copies, and remove any items they believe may provide evidence of an offence under the Act. They are also empowered to require explanations from data controllers or processors regarding records or documents and may remove equipment, commodities, or products that are used in contravention of the law **Data Protection Acts section 8(1)(a)–(g)).** Additionally, **Section 8(5)** [68]obliges inspectors to issue a receipt for any item removed and return it as soon as practicable after the inspection is complete.

Despite these detailed provisions, there are practical challenges in enforcement. One major concern is the lack of clear guidance on how inspectors should handle disputed property. While the Act allows inspectors to remove documents and equipment, it does not provide a step-by-step procedure for managing items when ownership is contested or when the property may be needed urgently for business operations. This leaves room for uncertainty and potential disputes between data subjects or organizations and the inspectorate.

Another limitation is the potential for misuse of inspector powers. The Act grants broad authority, including removing property and accessing sensitive records, but it does not explicitly define the checks and balances needed to ensure inspectors do not act beyond their mandate, for example, the absence of clear monitoring mechanisms could lead to delays in returning seized property, which may disrupt business operations or compromise the rights of individuals whose property is held for investigation.[69]

These gaps highlight the tension between enforcing compliance and protecting the rights of data subjects and businesses. Effective enforcement requires inspectors to have strong powers, but these powers must be accompanied by safeguards to prevent abuse. Without such safeguards, there is a risk that enforcement could become arbitrary or negatively impact the public's trust in the system. Therefore, while Section 8 provides a

[67] Act No. 3 of 2021
[68] Ibid
[69] Understanding Data Protection and Privacy Laws in Zambia https://generisonline.com/understanding-data-protection-and-privacy-laws-in-zambia (Accessed on 20/04/2025)

solid legal basis for inspectors' powers, the lack of detailed operational procedures and oversight mechanisms remains a significant limitation in Zambia's cyber security and data protection framework.[70]

3.3 ARRESTS AND SEIZURE OF PROPERTY

The **Data Protection Act**[71] gives inspectors wide enforcement powers, including the authority to arrest people and seize property. **Section 9** states that an inspector may arrest a person without a warrant if there are reasonable grounds to believe that the person has committed an offence under the Act, is about to commit an offence, or is obstructing an inspector from doing their job. This section also requires that anyone arrested must be taken to a police station without delay. The intention of this provision is to allow quick action in situations where waiting for a warrant may frustrate justice or allow offenders to escape responsibility.

In addition to arrest powers, **Section 10**[72] gives law enforcement officers the right to seize and detain property that is suspected of being used to commit offences under the Act. This includes documents, equipment, or any other item linked to the suspected offence. The property remains in detention until a court decides how it should be disposed of. While this helps secure evidence, it also creates challenges when items are seized for long periods, especially when they are essential for business operations.

To balance these strong powers, **Section 11**[73] introduces safeguards. It requires law enforcement officers to restore property without delay if the person is found not guilty or if the case is withdrawn. However, difficulties arise when the owner cannot be found or refuses to take back the property. In such cases, the officer may apply to the court for forfeiture, and the law provides that a notice should be published in the Gazette and in a daily newspaper. If no one claims the property within three months, it is forfeited to the State. While this provision gives a process for final disposal, it is often slow and complicated, which can negatively affect the rights of businesses and individuals.

---

[70] Michael Pisa , Pam Dixon, and Ugonma Nwankwo. Why Data Protection Matters for Development: The Case for Strengthening Inclusion and Regulatory Capacity. Center for Global Development. 2021

[71] Act No. 3 of 2021

[72] Act No. 3 of 2021

[73] Ibid

These sections show that while the Act[74] provides inspectors with strong powers, it is not equally strong in giving clear procedures for accountability. For example, there are no guidelines on how disputes over seized property should be resolved quickly, and there is a risk of abuse when arrests are made without warrants. This gap undermines trust in the system and highlights the need for stronger oversight mechanisms.

3.4 OFFENCES, PENALTIES, AND COMPENSATION

The **Data Protection Act No. 3 of 2021** sets out offences, penalties, and compensation measures that are central to Zambia's legal framework on cyber security and cyber crimes. These provisions aim to safeguard the rights of data subjects while ensuring accountability for data controllers and processors who mishandle personal data. **Sections 72 to 77** [75]are particularly important in this regard.

Section **73(1)** makes it an offence for any person to unlawfully disclose sensitive personal data to another person. This provision is vital because sensitive personal data, such as health records or financial details, if leaked, can cause serious harm to individuals. The penalty for this offence under Section **73(2)[76]** is a fine not exceeding **two hundred thousand penalty units** or imprisonment for up to **two years**, or both. This penalty shows that Parliament treats the protection of sensitive information as a serious matter that requires both criminal and financial consequences.

Beyond disclosure offences, **Section 76** [77]addresses corporate accountability. It provides that when a body corporate or unincorporated body commits an offence, and it is shown that the director, manager, or shareholder consented to or had knowledge of the offence, such officers can also be held personally liable. This provision prevents corporate leaders from hiding behind the legal entity of a company and ensures that responsibility extends to individuals who influence the actions of the organization.

The Act also provides for remedies to individuals whose rights have been violated. **Section 72** [78]states that a data subject who has suffered damage due to an infringement of their rights under the Act may receive **compensation** from the data controller or

[74] Ibid
[75] Act No. 3 of 2021
[76] Ibid
[77] Ibid
[78] Ibid

processor, as determined by a court of competent jurisdiction.[79] This civil remedy is essential because it allows individuals to recover losses caused by mishandling of their personal data. Compensation can cover both financial and non-financial harm, such as reputational damage.

However, while these provisions look strong on paper, their enforcement faces challenges. Sections **8 to 11**[80] give inspectors broad powers to seize property, remove documents, and make arrests, yet the Act does not provide detailed safeguards to prevent misuse of these powers. For instance, Section **11**[81] requires the restoration of seized property if a person is not guilty, but it is not clear how disputes over ownership are resolved or how delays can be prevented. This creates practical difficulties for businesses and individuals seeking to recover wrongfully seized property.

3.5 CODES OF CONDUCT AND ENFORCEMENT CHALLENGES

The Data Protection Act[82] gives the **Data Protection Commissioner** the power to prepare and publish a code of conduct. **Section 78(1)**[83] clearly states that the Commissioner may prepare a code of conduct for data controllers, processors, and auditors. Once published, this code becomes binding and must be followed. Its aim is to set clear standards for how personal data should be collected, processed, stored, and transmitted. It is also designed to make sure that those who handle personal data act in a way that respects the rights of data subjects.

The law highlights some of the important areas that must be covered in the code. **Section 78(2)**[84] lists confidentiality, fair representation of services, transparency in data processing, and the need to provide information to data subjects in a simple and accessible way. For example, a company collecting personal data is expected to explain clearly how it will use the information and must avoid misleading or hiding important

[79] Preston Mwiinga, Sylvester Mugala and Nadia Mungala, 'Cybersecurity and Digital Transformation in Zambia: Enhancing Awareness for a Secure Future' (2024) *International Journal of Functional Informatics and Personalised Medicine* 1(1) 6

[80] Act No. 3 of 2021

[81] Act No. 3 of 2021

[82] Ibid

[83] Ibid

[84] Ibid

details.[85] Once the Commissioner publishes the code in the Gazette or on an official website, it takes effect immediately according to **Section 78(3).**[86] If anyone violates the code, Section 78(5) makes it an offence punishable by a fine of up to two hundred thousand penalty units, imprisonment for up to two years, or both.

While this looks strong in theory, in practice the effectiveness of the code depends on how well it is enforced. One of the main challenges is that the Act gives broad powers to inspectors under **Sections 8 and 9**, including the power to remove documents, seize property, and even arrest without a warrant. However, there are no detailed procedures on how inspectors should use these powers in relation to the code of conduct. For example, when an inspector seizes property under Section 10, the Act does not fully explain how disputes over ownership will be resolved quickly, even though Section 11 talks about restoration. This gap creates uncertainty for businesses and individuals, and it can lead to abuse if inspectors act without proper oversight.

To build trust, the law needs to go beyond granting powers and punishments. There must be practical guidelines to help inspectors enforce the code fairly. Training inspectors, setting up independent monitoring bodies, and creating clear complaint procedures could help reduce abuse and improve public trust.[87] Without these safeguards, the strong provisions in **Section 78** [88]may not achieve their intended purpose of protecting data subjects and promoting accountability in Zambia's digital environment.

3.6 THE CYBER SECURITY ACT NO. 3 OF 2025

The growth of digital technologies has created both opportunities and risks. As more government institutions, businesses, and individuals rely on digital systems, the need for strong legal safeguards against cyber threats has become urgent. In Zambia, the legal response to these challenges has been consolidated in the Cyber Security Act No. 3 of 2025. This Act repealed the earlier Cyber Security and Cyber Crimes Act of 2021 and introduced a new framework aimed at protecting critical information infrastructure,

[85] Elijah Muntanga and Tuesday Bwalya, 'Electronic records management in government departments and parastatals in Zambia' (2024) 9 *IP Indian Journal of Library Science and Information Technology* 119

[86] Act No. 3 of 2021

[87] Preston Mwiinga, Sylvester Mugala and Nadia Mungala, 'Cybersecurity and Digital Transformation in Zambia: Enhancing Awareness for a Secure Future' (2024) International Journal of Functional Informatics and Personalised Medicine 1(1) 6

[88] The Data Protection Act No. 3 of 2021

preventing cyber incidents, and ensuring accountability in enforcement. The Act also establishes institutions and procedures that are meant to strengthen cyber resilience while balancing the rights of individuals and the responsibilities of controllers and service providers.[89]

A key feature of the new Act is the establishment of the Zambia Cyber Security Agency under **section 3.** [90]The Agency, which operates under the Office of the President, is responsible for coordinating cyber security matters across the Republic. Its functions, outlined in section 4, include responding to cyber incidents, identifying and protecting critical information infrastructure, licensing cyber security service providers, and issuing codes of practice and standards. This institutional framework reflects the importance of placing cyber security at the highest level of government oversight, given its link to national security, economic stability, and the protection of personal rights.

The Act places strong emphasis on the protection of critical information and infrastructure. **Sections 8 to 11** [91]provide for the designation of certain sectors as critical, including defence, finance, health, transport, energy, and information technology. Once infrastructure in these sectors is designated as critical, controllers must register it with the Agency and comply with baseline security requirements. Failure to register or comply is treated as a serious offence, punishable by fines or imprisonment. This focus on critical infrastructure is essential because disruption in these sectors could have wide-ranging impacts on national security and public welfare. The law also requires hosting of critical information within Zambia unless authorised otherwise, as provided under **section 12**[92]. This requirement is linked to national sovereignty and the need to avoid over-reliance on foreign jurisdictions that may not provide adequate protection.

The framework also includes strong enforcement powers. Section 18 empowers inspectors to investigate cyber threats and incidents once they meet a certain severity threshold. Inspectors may request documents, question controllers, direct remedial action, and in some cases, enter premises with a warrant to seize or examine computer systems. These provisions are similar in spirit to the Data Protection Act, which also gave

[89] Act No. 3 of 2025
[90] Act No. 3 of 2025
[91] Ibid
[92] Ibid

broad powers to inspectors. However, **the Cyber Security Act** [93]tries to strike a balance by requiring warrants in certain cases and mandating the return of seized equipment after investigations are complete. Despite this, questions remain on how effectively these provisions can be enforced, especially in relation to oversight and accountability of inspectors.

Another important part of the Act concerns the handling of seized property**. Sections 59 to 61**[94] provide that law enforcement officers may, with a warrant, seize computers or systems that contain evidence of an offence. Where the accused is acquitted or charges are dropped, the property must be restored within thirty days. If the owner cannot be found, the officer must apply to court for an order of forfeiture. This provision is a step forward because it creates a judicial safeguard. Yet, as highlighted in the statement of the problem, challenges may still arise if there is ambiguity in the restoration process or delays in returning seized property, which may affect businesses and individuals negatively.

The Act also provides remedies and safeguards for those affected by enforcement decisions. Under **section 58,** [95]a person aggrieved by a decision of the Agency may appeal to the High Court within thirty days. This ensures that there is judicial oversight over the actions of the Agency. Furthermore, **section 62** [96]states that evidence obtained by unlawful interception is not admissible in court, unless the court grants leave after weighing the circumstances. These provisions highlight the law's recognition of the need to balance enforcement with protection of rights such as privacy and fair trial.

Despite its strengths, the Act faces challenges that mirror those in the **Data Protection Act**.[97] The broad investigative powers granted to inspectors and law enforcement officers raise concerns about potential abuse if there are no clear operational guidelines. For example, although warrants are required in some cases, other provisions allow inspectors to request sensitive data with written notice, which may be misused without proper monitoring. In addition, while the law provides for restoration and appeals, it does not go

[93] Ibid
[94] Act No. 3 of 2025
[95] Act No. 3 of 2025
[96] Ibid
[97] The Data Protection Act No. 3 of 2021

far enough in setting out practical steps, timeframes, and oversight mechanisms that would guarantee accountability. This gap is significant because enforcement is only as strong as the trust that citizens and businesses have in the institutions carrying it out.

3.7 CYBER CRIMES ACT NO. 4 OF 2025

Cyber security and cyber crimes are increasingly critical in Zambia as the use of computers, networks, and digital platforms grows across all sectors. The Zambian government has recognized the need to protect information systems and data from illegal access, manipulation, and misuse. This recognition led to the enactment of the **Cyber Crimes Act**,[98] which provides a comprehensive legal framework aimed at preventing cyber offences, ensuring accountability, and protecting critical information infrastructure. The Act criminalizes a wide range of cyber activities, with penalties designed to deter potential offenders and maintain trust in digital systems.

The Act prohibits unauthorized access to computer systems and data. Section 3 makes it an offence to intentionally infringe any security measure or monitor another person's computer system without lawful authority. This provision is crucial because it protects both individuals and businesses from intrusion, which is a growing concern in a digital economy. Similarly, **Section 4** [99]criminalizes unauthorized interference with computer data or systems, such as modifying, destroying, or obstructing the use of data. These offences recognize the importance of data integrity and the potential economic and social harm that can result from cyber disruptions.

Protection of critical information is another key focus of the Act. **Sections 5 and 6** [100]make it illegal to disclose, transmit, or possess data relating to critical information infrastructure without proper authority. The law emphasizes severe penalties, including imprisonment of up to fifteen years, reflecting the potential national security implications of such crimes. The inclusion of these provisions is particularly important because, as seen in the statement of the problem, weak enforcement mechanisms in other areas, like data protection, can undermine public trust. By criminalizing unauthorized possession and

[98] Cyber Crimes Act No. 4 of 2025
[99] Ibid
[100] Cyber Crimes Act No. 4 of 2025

communication of critical data, the Cyber Crimes Act aims to establish clear boundaries and responsibilities.

The Act also addresses illegal acquisition of sensitive data and trade secrets. **Section 7** [101]prohibits obtaining confidential or proprietary information through computers without lawful authority. **Section 8** [102]criminalizes the introduction of malicious software into another person's computer system, highlighting the importance of safeguarding digital infrastructure from intentional harm. These provisions complement the overall goal of cyber security, which is to ensure that digital systems remain reliable, trustworthy, and free from malicious interference.

Cyber fraud, misrepresentation, and extortion are equally targeted. **Sections 12 and 13** [103]make it an offence to input false data, manipulate electronic systems, or engage in extortion through digital means. By including these offences, the law acknowledges that cyber crimes are not limited to technical intrusion but also include schemes designed to deceive or coerce victims for financial or personal gain. Sections 14 to 16 extend protections to identity-related crimes, child exploitation, and online grooming, demonstrating a comprehensive approach that safeguards both individuals and society from digital threats.

The Act further addresses the misuse of computer systems for harassment, humiliation, or emotional distress. **Section 22** [104]criminalizes the dissemination of obscene, vulgar, or false information intended to harm another person. Additionally, cyber attacks and cyber terrorism are directly prohibited under **Sections 23 and 24.** [105]These provisions recognize that cyber crimes can have far-reaching consequences, affecting not only individuals but also the security and stability of national infrastructure. **Section 25** [106]imposes severe penalties for offences that disrupt critical infrastructure, emphasizing the importance of digital resilience for the Republic.

While the Cyber Crimes Act provides a robust legal framework, enforcement remains a challenge. The Act gives authorities clear powers to investigate and prosecute cyber

[101] Cyber Crimes Act No. 4 of 2025
[102] Ibid
[103] Ibid
[104] Cyber Crimes Act No. 4 of 2025
[105] Ibid
[106] Ibid

offences, but practical implementation requires skilled personnel, technological tools, and monitoring mechanisms. The statement of the problem in this thesis highlights similar challenges in data protection, where inspectors' powers can be abused due to lack of oversight. In cyber security, the complexity of digital offences and the anonymity provided by online systems can make enforcement difficult. Therefore, the effectiveness of the Act depends not only on its legal provisions but also on operational capacity, inter-agency coordination, and public awareness.

3.8 CONCLUSION

Zambia's legal framework for cyber security and cybercrimes provides comprehensive measures to prevent, detect, and punish offences while protecting critical information and infrastructure. The Data Protection Act, Cyber Security Act, and Cyber Crimes Act collectively create a system where inspectors and agencies have broad powers to monitor, investigate, and enforce compliance, and where penalties and remedies aim to deter misconduct. However, the effectiveness of these laws depends on clear operational guidelines, oversight mechanisms, and proper enforcement capacity. Gaps remain in accountability, timely restoration of seized property, and monitoring of enforcement actions, which could undermine public trust and compliance.

CHAPTER FOUR

HUMAN RIGHTS SAFEGUARDS IN ENFORCEMENT- RELATED PROVISIONS OF THE ZAMBIAN DATA PROTECTION ACT WITH THOSE IN COUNTERPART LEGISLATION IN NIGERIA, SOUTH AFRICA, KENYA, AND THE UNITED KINGDOM

4.0 INTRODUCTION

This chapter compares how Zambia's Data Protection Act protects human rights during enforcement with how other countries Nigeria, South Africa, Kenya, and the United Kingdom handle similar situations. The goal is to show how these countries balance the power to enforce data protection laws with the need to respect privacy, dignity, and due process. In Zambia, the law gives inspectors wide powers to enter premises, inspect documents, and seize items, but it does not always require a judge's warrant or prior authorization before such actions. This creates a risk of abuse or intrusion into people's privacy. In contrast, countries like Nigeria, South Africa, Kenya, and the United Kingdom have stronger safeguards. Their laws clearly state that enforcement officers must obtain a court warrant before entering private property or conducting searches. They also provide rights of appeal, compensation for those harmed by wrongful enforcement, and accountability measures for officers who misuse their powers. These systems ensure transparency, proportionality, and fairness during enforcement. Therefore, this chapter explores how Zambia can learn from these countries to strengthen its own human rights protections in data enforcement by adding judicial oversight, clear appeal procedures, and accountability mechanisms for misuse of power.

4.1 HUMAN RIGHTS SAFEGUARDS ON DATA PROTECTION IN SOUTH AFRICA

The South African **Protection of Personal Information Act**[107] (POPIA) requires that enforcement officers get a judicial warrant before they can enter premises, search, seize materials or equipment. Under **Section 82**[108] a warrant must be issued by a judge of the High Court, a regional magistrate or a magistrate, after being satisfied on oath by the Regulator that there are reasonable grounds to suspect that an offence under POPIA is being committed or that protection of personal information is being interfered with, and

[107] Act No. 4 of 2013
[108] Ibid

that evidence is likely to be found on the premises. Moreover, Section 83 places further limits: the court must ensure the occupier has been given notice demanding entry under reasonable hour, that access was unreasonably refused or that a request for cooperation was unreasonably refused, and that the occupier had the chance to be heard before the warrant is issued (unless in urgent cases). This ensures enforcement is not arbitrary.

During execution of a warrant under **Section 84**, the law requires that the search be done at reasonable hours, that the occupant be shown the warrant (or the copy left visibly), that receipts be given for seized items, and that the rights of dignity, freedom, security and privacy be respected. Also, individuals being questioned must be told of their right to legal representation. Self-incriminating statements given under such searches are generally not admissible.[109]

By comparison, **Zambia's Data Protection Act**[110] allows inspectors broad powers of entry, seizure, question, etc., but does not require a warrant from a magistrate or judge before entry/search/seizure in many of its provisions. This means fewer formal checks before enforcement actions that intrude on property or privacy.

4.2 APPEALS, REMEDIES AND TRANSPARENCY

POPIA gives strong procedural rights to people affected by decisions of the Regulator. Under **Section 97**[111], any "responsible party" (entity or person who has been served an information or enforcement notice) may appeal within 30 days to the High Court to set aside or modify the notice. A complainant (person who raised a complaint) also has a right under the same or similar process (within 180 days) to appeal decisions against them. Enforcement notices themselves must contain information about the right of appeal under Section 95.[112] The law prevents sudden surprises: an enforcement notice cannot demand compliance before the appeal period lapses in many cases, unless urgency is justified and explained.

[109] Act No. 4 of 2013
[110] Act No. 3 of 2021
[111] Act No. 4 of 2013
[112] Ibid

There are also civil remedies: under **Section 99**[113], data subjects (or the Regulator on behalf of data subjects) may take civil action for damages when POPIA is breached. This covers non-financial harms too (like damage to reputation etc.).

Additionally, transparency is built in: Section 90 (information notices) requires that notice include particulars of the appeal right under **Section 97. Section 94** [114]obliges the Regulator to inform both complainant and responsible parties about developments during an investigation and results. These ensure that parties know what is happening, and have opportunity to respond.

Zambia's law does have appeal mechanisms (you mentioned appeal to High Court), but lacks many of the advance notice requirements, judicial pre-approval of searches, clear requirements for transparency during enforcement, and detailed civil damages options comparable to what POPIA spells out.

4.2.1 Protection of privilege and fairness

POPIA has specific protection for privileged communications. Under **Section 86** and **Section 87**,[115] communications between a legal adviser and client are exempt from search and seizure under a warrant, or if a material is seized which contains privileged information, the person executing the warrant must request the Registrar of the High Court to attach and remove that material for safe custody until the court rules whether it is privileged. Also, the law demands that searches be done with "strict regard for decency and order, and with regard to each person's right to dignity, freedom, security and privacy." Before questioning a person found during execution of the warrant, the person must be advised of their right to legal assistance. The law also ensures that statements which are self-incriminating are not admissible (unless in very specific types of proceedings).

These kinds of protections for dignity, privilege, and self-incrimination are not as clearly spelled out in Zambia's Act with respect to enforcement and inspector powers. Zambia's law gives inspectors authority to remove documents, equipment, etc., but does not

[113] Ibid
[114] Ibid
[115] Act No. 4 of 2013

mandate legal representation, judicial control over searches, or protection of privileged communications in this strong a way.

4.2.2 Minimal intrusion, proportionality & preventing abuse

POPIA has a strong sense that any enforcement action must be the minimum needed and proportional. The warrant regime under **Sections 82-83**[116] ensures that before intrusion, the court evaluates whether less intrusive means have been tried (notice, request for access) or whether urgency justifies bypassing notice. This aligns enforcement with human rights principles (privacy, property).

Also, when inspectors or the Regulator act, the execution of warrants under **Section 84** [117]includes limits on when entry happens (reasonable hour), ensures copy of warrant or leaving of such visible, requiring that items seized be receipted, etc., that retention of seized items be only for as long as necessary, and that the occupier is given copies of documentation seized as far as possible without delay.

POPIA also has complaint-procedures under **Sections 74-76**[118], pre-investigation proceedings under **Section 79**[119], and obligations for Regulator to inform parties and allow response. These all contribute to making sure enforcement is not abused.

In Zambia's law, while there are powers to enter, inspect, seize and even arrest, there are fewer requirements that these powers must be judicially authorized or that occupiers have chance to contest before or during execution; fewer detailed procedural protections, fewer constraints on how long property may be kept, or formal protections of privilege or self-incrimination in the same way.

4.3 HUMAN RIGHTS SAFEGUARDS IN ENFORCEMENT IN NIGERIA

Nigeria's Act explicitly ties its enforcement powers to constitutional protections of privacy under **Section 37 of the Nigerian Constitution**[120] which provides that the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected, therefore this provision requires that where enforcement officers need to enter premises or carry out searches/seizures,

[116] Ibid
[117] Act No. 4 of 2013
[118] Ibid
[119] Ibid
[120] Constitution of the Federal Republic of Nigeria 1999

they must first obtain a warrant from a judge. For example, under the Nigeria **Data Protection Act Section 58**[121] the Commission must apply ex parte to a Judge in Chambers for a warrant "for the purpose of obtaining evidence in relation to an investigation." The judge may issue the warrant only after being satisfied of certain conditions, such as that an offence is being committed or is likely to be committed, or to prevent interference with investigation.[122]

Zambia's Act allows inspectors appointed under **Section 7**[123]broad powers to enter premises, inspect documents, seize things, etc., but does not require obtaining a judicial warrant before doing so. There is risk of arbitrary entry, seizure or inspection in Zambia due to absence of a built-in requirement for prior judicial authorization. Thus, Nigeria's requirement of a judge's warrant acts as a key safeguard: it ensures oversight before rights of property, privacy and due process are invaded.

4.3.1 Right to appear in court, appeal & accountability

Nigeria's law provides explicit measures for individuals (and entities) affected by enforcement actions to seek redress in court. Under **Section 59**[124] ("Right to appear in court") and related legal proceedings (Part XI), there are provisions for representation in court, for seeking judicial review of enforcement decisions. For instance, a person subject to the powers granted by **Section 58**[125] can challenge wrongful searches or seizures, or misuse of power, in Federal High Court. The law also contains indemnity and restriction of execution, meaning the Commission's property cannot be seized in certain actions, and staff are protected in certain lawful acts.

By contrast, Zambia's **Act**[126]does include an appeal to the High Court if someone is aggrieved by the Data Protection Commissioner's decision. Under Zambia's Act, **Section 69**[127] provides that "A person who is aggrieved with the decision of the Data Protection Commissioner may appeal to the High Court within thirty days."

[121] Nigeria Data Protection Act No. 37 of 2023
[122] Ibid
[123] Act No. 3 of 2021
[124] Nigeria Data Protection Act No. 37 of 2023
[125] Ibid
[126] Act No. 3 of 2021
[127] Act No. 3 of 2021

However, Zambia's law lacks the stronger pre-entry warrant requirement and some of the safeguards around seizure/search powers present in Nigeria. Also, Zambia does not provide detailed limitations or judicial pre-authorisation for when inspectors may enter premises or seize property (outside courts' involvement via appeal after the fact), which may leave data subjects vulnerable.

4.3.2 Proportionality & limits, misuse prevention

Nigeria's Act has built-in restrictions meant to ensure that when enforcement officers act, they do not overreach. The warrant authorisation in **Section 58**[128] is limited to cases where the judge is satisfied certain conditions hold (e.g. reasonable suspicion, urgent need, evidence of an offence, risk of interference). This means that inspections, searches or seizures must be justified and proportionate to the risk or alleged wrongdoing. Also, **Section 58**[129] limits what can be seized (items connected with offences under the Act, devices holding relevant electronic data etc.), and how far one can go (e.g. requiring decryption only as allowed, requiring devices to be produced etc.) under a judicial warrant.

Nigeria's law also has provisions to punish misuse of powers: if persons misuse authority or act beyond what is authorised, there are legal consequences. There are indemnity provisions under **Section 57** [130]but only where lawful, and legal accountability remains for wrongful or excessive actions.

Zambia's Act, while strong in giving inspectors powers, does not contain a similar mandate that enforcement must be "necessary only to the extent required" in the same explicit way that Nigeria does via judicially approved warrants. Nor are there detailed provisions in Zambian law for judges to control search/seizure or oversight prior to enforcement action. This gap means there is less legal check on proportionality before intrusion.

4.4 HUMAN RIGHTS SAFEGUARDS IN ENFORCEMENT IN KENYA

In Kenya, the **Data Protection Act** [131]gives the Office of the Data Protection Commissioner (ODPC) powers to enter and search premises, but only after obtaining a

[128] Nigeria Data Protection Act No. 37 of 2023
[129] Ibid
[130] Nigeria Data Protection Act No. 37 of 2023
[131] Data Protection Act No. 24 of 2019

warrant from a Court. **Section 60 of Kenya's Act** [132]states: "The Data Commissioner, upon obtaining a warrant from a Court, may enter and search any premises for the purpose of discharging any function or exercising any power under this Act."

This means that before inspectors or authorized officers can force their way into buildings or seize property, they need prior judicial authorization. That protects individuals and businesses from arbitrary intrusion. Zambia's Act[133] allows inspectors wide powers of entry, inspection, seizure, and even arrest without always requiring a warrant or specific judicial approval. This contrast is important for protecting rights to privacy, property and due process.

4.4.1 Right of Appeal and Remedy

Kenya's law explicitly provides an avenue for individuals or entities who are disagreed with administrative or enforcement actions. Under **Section 64 of Kenya's Act**:[134] *"A person against whom any administrative action is taken by the Data Commissioner, including in enforcement and penalty notices, may appeal to the High Court."*

Kenya's framework also provides for **compensation** to data subjects. **Section 65**[135]allows someone who suffers damage due to contravention of the Act to get compensation from the data controller or processor.[136]

Moreover, the Kenya law gives limits and procedural clarity for enforcement notices. **Section 58**[137]requires that an enforcement notice **must** include what provision is breached, what remedies are needed, a time period (not less than 21 days) for compliance, and it must state the right of appeal.

In addition, Kenya's regulations (Data Protection (Complaints Handling Procedure and Enforcement) Regulations, 2021)[138] reinforce these rights. For example, if someone receives an enforcement notice, there is a right to appeal to the High Court within thirty days.

---

[132] Ibid

[133] The Data Protection Act No. 3 of 2021

[134] Data Protection Act No. 24 of 2019

[135] Ibid

[136] Ibid

[137] Data Protection Act No. 24 of 2019

[138] These Regulations may be cited as the Data Protection (Complaints Handling Procedure and Enforcement) Regulations. Legal Notice 264 of 2021

4.4.2 Transparency, Proportionality, and Penalties

Kenya's Act sets out factors to consider when imposing penalties: the nature and gravity of failure, duration, whether the person acted negligently or intentionally, cooperation, previous failures, categories of data involved, etc. These are in **Section 62**[139]. This ensures penalties are proportionate and dissuasive.in addition, there are offences for obstructing the Commissioner in **Section 61** and rules on wrongful disclosure of personal data in **Section 72.**[140]

Compared to Zambia, which grants broad powers (arrest without warrant, seizure without detailed procedural checks), Kenya's law introduces more constraints and procedural steps, making enforcement less likely to abuse rights.

4.5 HUMAN RIGHTS SAFEGUARDS IN ENFORCEMENT IN UNITED KINGDOM

The United Kingdom's Data Protection Act, 2018 (DPA 2018), strengthens individual rights and ensures that data protection enforcement does not violate human dignity or privacy. It was enacted to align with the European Union's General Data Protection Regulation (GDPR), which sets high standards for fairness, transparency, and accountability in handling personal data. The Act provides several safeguards that Zambia's law currently lacks, especially in ensuring independent.

4.6 INDEPENDENT ENFORCEMENT AND OVERSIGHT

Under **Section 114 of the DPA 2018**,[141] the **Information Commissioner's Office (ICO)** is established as an independent authority responsible for promoting and enforcing compliance with data protection principles. The ICO has broad powers to investigate, issue enforcement notices, and impose penalties for non-compliance. However, unlike Zambia's inspectorate system under **Section 7 of the Data Protection Act**,[142] the ICO is **fully independent of the executive branch**. This independence prevents government interference and promotes public trust in data regulation.

The Act ensures that inspections or searches are not arbitrary. **Section 147**[143] provides that the ICO can only enter and inspect premises under a **warrant issued by a judge of**

[139] Data Protection Act No. 24 of 2019
[140] Data Protection Act No. 24 of 2019
[141] Data Protection Act 2018
[142] Act No. 3 of 2021
[143] Data Protection Act 2018

the High Court or Circuit Court, based on reasonable grounds. The judge must be satisfied that there is evidence of non-compliance or obstruction before granting the warrant. This safeguard prevents inspectors from abusing power or conducting random searches. By contrast, Zambia's Act allows inspectors to enter premises and seize property under **Section 8**[144]without requiring prior judicial authorization, increasing the risk of abuse and violating the constitutional right to privacy.

4.7 APPEALS, DUE PROCESS, AND HUMAN RIGHTS PROTECTION

Another strong safeguard in the UK law is the **right of appeal**. Under **Section 173**, any person who receives an enforcement notice, penalty notice, or information notice may appeal to the **First-tier Tribunal (Information Rights)**. This tribunal operates independently from the ICO and provides a fair process for reviewing enforcement actions. The law further requires, under **Section 175**,[145] that the individual or organization affected must be notified in writing of the reasons for the decision and given an opportunity to respond before enforcement is carried out.

These procedural guarantees are grounded in **Article 8 of the European Convention on Human Rights (ECHR)**,[146] which protects the right to privacy and family life. Therefore, all enforcement actions by the ICO must be proportionate and justifiable. If a person feels their privacy has been violated, they can take the matter to court under **Section 168**,[147]which gives them a right to compensation for material and non-material damages caused by breaches of data protection rules.

This system contrasts with Zambia's framework, where there are no explicit appeal provisions against inspectors' decisions, and the Act lacks clear procedures for notifying individuals of enforcement actions. This absence weakens accountability and can lead to arbitrary decisions without recourse.

4.8 ACCOUNTABILITY AND PENALTIES FOR ABUSE OF POWER

The UK Data Protection Act also includes strict provisions to ensure accountability among enforcement officers. **Section 196** makes it a criminal offence for any person, including

---

[144] Act No. 3 of 2021

[145] Data Protection Act 2018

[146] **European Convention on Human Rights (ECHR).** *Article 8 – Right to respect for private and family life.* Available at: https://www.echr.coe.int

[147] Data Protection Act 2018

officers of the ICO, to unlawfully disclose personal data obtained during investigations. The penalty for this offence is a fine or imprisonment, depending on the severity. Additionally, **Schedule 15** requires the ICO to act fairly, proportionately, and in a way that respects human rights when exercising enforcement powers.

Zambia's Data Protection Act, while establishing offences under **Sections 72 to 77**[148], does not directly criminalize abuse of power or misuse of data by inspectors. This creates a gap in accountability that the UK law resolves by making misuse of authority a punishable offence. Furthermore, **Section 132** of the UK Act[149] requires regular reporting by the ICO to Parliament, ensuring public transparency and continuous oversight of enforcement actions another safeguard Zambia's law lacks.

4.9 CONCLUSION

The comparison shows that Zambia's Data Protection Act still falls short of meeting strong human rights standards during enforcement. While it provides a general right of appeal to the High Court, it lacks detailed safeguards that prevent abuse, such as mandatory judicial warrants, advance notice to affected persons, and strict limits on searches and seizures. Nigeria's and Kenya's laws stand out for requiring judges to authorize enforcement actions, ensuring that privacy and property rights are not violated without proper cause. South Africa's POPIA adds strong procedural rights, transparency, and protection for privileged communication, while the United Kingdom's Data Protection Act, 2018, further enforces accountability through independent oversight by the Information Commissioner's Office and criminal penalties for misuse of power. These countries show that it is possible to enforce data laws effectively while still upholding human rights and fairness. Zambia can strengthen its framework by adopting these best practices especially judicial control, proportionality, and transparency to ensure that data enforcement respects human dignity and builds public trust in the country's data protection system.

[148] The Data Protection Act No. 3 of 2021

[149] Data Protection Act 2018

CHAPTER FIVE

CONCLUSIONS AND RECOMMENDATIONS

5.0 INTRODUCTION

This chapter was based on drawing final conclusions and providing recommendations from the entire study on Zambia's Data Protection Act and its enforcement framework. It summarises the findings from previous chapters, showing that while Zambia has made progress with laws like the Data Protection Act No. 3 of 2021, the Cyber Security Act No. 3 of 2025, and the Cyber Crimes Act No. 4 of 2025, there are significant gaps in enforcement, accountability, and protection of human rights. The study found that inspectors under Sections 7 to 11 of the Data Protection Act have broad powers to enter premises, seize property, and make arrests, but the Act lacks judicial oversight, detailed procedures, and safeguards to prevent abuse. Comparative analysis with Nigeria, South Africa, Kenya, and the United Kingdom revealed that these countries enforce data protection while protecting privacy, dignity, and due process through judicial warrants, clear appeal mechanisms, proportional enforcement, and independent oversight, as seen in Sections 58 of Nigeria's Act, Sections 82-84 of South Africa's POPIA, Section 60 of Kenya's Act, and Sections 132 and 196 of the UK DPA 2018. Based on these lessons, the chapter recommends establishing independent oversight, clear procedures for seized property, judicial control of enforcement, accountability measures for inspectors, operational training, and enhanced procedural safeguards and appeal rights to strengthen Zambia's enforcement framework, protect human rights, and build public trust.

5.1 FINDINGS AND CONCLUSIONS

5.1.1 CHAPTER ONE

Chapter one gave a general overview of the topic and set the foundation on a comparative analysis of enforcement - related provisions in the data protection act in zambia with those in counterpart legislation in South Africa, Kenya, Nigeria, and the United Kingdom. It gave a brief background to the study; further, it looked at the statement of the problem, objectives of the study, research questions and significance. Then, a literature review was given stating how the study differs from other authors and finally the methodology of the study.

5.1.2 CHAPTER TWO

This chapter was based on explaining the meaning of cybersecurity and cybercrime and how laws and international instruments help protect people, data, and systems from online threats. The findings show that cybersecurity is not only about using technology like firewalls and encryption but also about creating awareness, enforcing laws, and building cooperation across countries. Cybercrime continues to grow because of the easy access to technology, anonymity on the internet, and weak security systems. The United Nations Convention Against Cybercrime, under Articles 1, 3, 6, and 7–13, provides rules for preventing, investigating, and prosecuting cyber offenses while respecting human rights. Similarly, the African Union's Malabo Convention, especially Articles 24 to 31, guides African countries to make strong national cybersecurity laws, promote a culture of safety, and work together to fight cyber threats.

This chapter shows that the fight against cybercrime requires strong laws, international cooperation, and public awareness. Both the United Nations Convention and the Malabo Convention help countries build safer digital spaces while protecting individual freedoms. By following these frameworks, societies can reduce cyber risks and make online systems more secure and trustworthy for everyone.

5.1.3 CHAPTER THREE

This chapter was based on examining the legal framework that governs cyber security and cyber-crimes in Zambia. The findings show that Zambia has made significant progress through three main laws: the Data Protection Act No. 3 of 2021, the Cyber Security Act No. 3 of 2025, and the Cyber Crimes Act No. 4 of 2025. These laws collectively protect personal information, critical infrastructure, and digital systems. They give inspectors and law enforcement officers powers to monitor, investigate, arrest, and seize property, as provided under Sections 7 to 11 of the Data Protection Act and Sections 59 to 61 of the Cyber Security Act. The findings also reveal that while these laws are strong in providing authority to inspectors, they lack detailed guidance on how such powers should be used fairly, creating risks of abuse and reducing public confidence in the system.

The findings further show that Zambia's framework has clear penalties for offences like unauthorized access, data breaches, cyber fraud, and identity theft, as provided under

Sections 3 to 8 and 12 to 16 of the Cyber Crimes Act No. 4 of 2025. These provisions play a key role in preventing misuse of technology and protecting citizens' rights online. The inclusion of compensation rights under Section 72 of the Data Protection Act allows victims to seek redress, showing that the law values accountability. However, practical enforcement challenges remain, especially in monitoring inspectors, resolving disputes over seized property, and ensuring quick restoration when a person is acquitted or found not guilty. These challenges affect how well the law achieves its goal of fairness and justice in digital governance.

This chapter shows that Zambia's legal framework for cyber security and cyber crimes is well-structured and provides a strong foundation for protecting individuals, businesses, and national systems from digital threats. However, for these laws to be fully effective, there must be stronger oversight, clear operational guidelines, and better training for inspectors and enforcement officers. Improving accountability, as required under Sections 7 to 11 of the Data Protection Act and Section 58 of the Cyber Security Act, would help build public trust and ensure that enforcement is fair and transparent. By addressing these practical issues, Zambia can create a safer and more trusted digital environment for all.

5.1.4 CHAPTER FOUR

This chapter was based on a comparative analysis of human rights safeguards in the enforcement provisions of Zambia's Data Protection Act and similar legislation in Nigeria, South Africa, Kenya, and the United Kingdom. The findings reveal that Zambia's law gives inspectors wide powers to enter premises, seize documents, and question individuals without always requiring prior judicial approval, detailed notice, or clear procedural safeguards. In contrast, countries like Nigeria, Kenya, and South Africa require judicial warrants before enforcement actions, provide clear appeal procedures, and protect privileges, privacy, and self-incrimination. The UK law goes further by establishing an independent enforcement authority, requiring judicial authorization for inspections, and imposing criminal penalties for abuse of power. These measures ensure proportionality, transparency, and accountability, which Zambia's Act currently lacks. While Zambia allows appeals to the High Court under Section 69, there is minimal guidance on advance

notice, limits on searches and seizures, or protection of privileged communications, creating risks of arbitrary enforcement and undermining public trust.

Zambia's Data Protection Act provides a legal basis for enforcing data protection, but it falls short in protecting human rights during enforcement. Lessons from Nigeria, Kenya, South Africa, and the UK show that judicial oversight, clear procedural safeguards, transparency, and accountability mechanisms are essential to prevent abuse of power and uphold privacy and dignity.

5.2 RECOMMENDATION

This research has revealed that Zambia's Data Protection Act provides broad powers to inspectors under Sections 7 to 10, but lacks strong safeguards for accountability, judicial oversight, and protection of individual rights. This is in contrast to countries like Nigeria, South Africa, Kenya, and the United Kingdom, where enforcement powers are balanced with human rights protections, including judicial warrants, appeal procedures, and independent oversight. The author therefore recommends the following:

1. Establish an Independent Oversight and Accountability Body

Zambia should create an independent body or strengthen an existing authority to monitor the work of inspectors under the Data Protection Act. This body should review complaints, investigate reports of abuse, and provide regular reports on how inspectors exercise their powers. It should also ensure that inspectors act lawfully and fairly when entering premises, seizing documents, or making arrests under Sections 7 to 10. This will promote transparency and prevent misuse of power.

2. Develop Clear Procedures for Handling and Returning Seized Property

The government should amend Sections 8 and 11 of the Data Protection Act to clearly explain how seized property or documents should be handled, stored, and returned. A specific time frame should be introduced for the return of items once an investigation is completed or when a person is acquitted. Clear rules should also guide how disputed property is managed when the owner cannot be found. These measures would help protect individuals' property rights and prevent unnecessary delays that affect businesses and citizens.

3. Provide Regular Training and Operational Guidelines for Inspectors

Inspectors should receive continuous training on how to exercise their powers responsibly and respect human rights during investigations. The Ministry of Technology and Science, working with the Data Protection Commission, should prepare detailed operational guidelines on how to conduct audits, make arrests, and seize property lawfully. This will help inspectors understand their limits, improve professionalism, and build public trust in data protection enforcement.

4. **Introduce Judicial Oversight for Enforcement Actions**

Zambia should amend the Data Protection Act to require inspectors to obtain a judicial warrant before entering premises, conducting searches, or seizing property. This would ensure that enforcement actions are justified, proportionate, and do not infringe on privacy or property rights, similar to the safeguards under Sections 82-84 of South Africa's POPIA, Section 58 of Nigeria's Data Protection Act, and Section 60 of Kenya's Data Protection Act. Judicial oversight would prevent arbitrary actions and build public trust in enforcement.

5. Strengthen Accountability Mechanisms for Inspectors

The law should include clear measures to hold inspectors accountable for abuse of power. This could involve criminal penalties or disciplinary action for unlawful conduct, independent monitoring of enforcement activities, and mandatory reporting of seizures and inspections, similar to the UK's DPA 2018 Sections 132, 196, and Schedule 15. Accountability would reduce misuse of authority and reassure the public that enforcement respects human rights.

6. Enhance Procedural Safeguards and Appeal Rights

Zambia should introduce clear procedures for advance notice of enforcement, protection of privileged communications, and timely return of seized property. Individuals and entities should have a defined right to appeal enforcement actions and seek compensation for wrongful seizures or breaches, as provided under Sections 97-99 of South Africa's POPIA, Sections 64-65 of Kenya's Data Protection Act, and Section 173 of the UK DPA 2018. These reforms would protect property and privacy rights, prevent abuse, and improve public confidence in data protection enforcement.

BIBLIOGRAPHY

JOURNAL ARTICLES

African Data Privacy (Springer International Publishing AG, 2016).

Bryant J, Africa in the Information Age: Challenges, Opportunities and Strategies for Data Protection and Digital Rights (Stan Tech 2021).

Freeze D, 'Cybercrime To Cost The World $9.5 Trillion USD Annually in 2024' (12 October 2023) Cybercrime Magazine.

Greenleaf G, 'Global Data Privacy Laws 2017: 120 National Data Privacy Laws, Including African Developments' (2018).

Lovet G, 'Fighting Cybercrime: Technical, Juridical and Ethical Challenges' (Virus Bulletin Conference, 2009).

Kapiyo V, Challenges in Implementing Data Protection Laws in Kenya (CIPESA Reports, 2019).

Kamleitner B and Mitchell V, 'Your Data Is My Data: A Framework for Addressing Interdependent Privacy Infringements' (25 July 2019) 38 Journal of Public Policy and Marketing.

Kemper G, 'Improving Employees' Cyber Security Awareness' (1 August 2019) Computer Fraud & Security.

Kim L, 'Cybersecurity Awareness: Protecting Data and Patients' (April 2017) Nursing Management.

Kholofelo K, The Impact of Data Localisation Laws on Trade in Africa (Mandela Institute 2022).

Michael Pisa, Pam Dixon and Ugonma Nwankwo, Why Data Protection Matters for Development: The Case for Strengthening Inclusion and Regulatory Capacity (Center for Global Development 2021).

Muntanga E and Bwalya T, 'Electronic Records Management in Government Departments and Parastatals in Zambia' (2024) 9(1) IP Indian Journal of Library Science and Information Technology 119.

Mwiinga P, Mugala S and Mungala N, 'Cybersecurity and Digital Transformation in Zambia: Enhancing Awareness for a Secure Future' (2024) 1(1) International Journal of Functional Informatics and Personalised Medicine 6.

Ndawana YM, State of the Internet Freedom in Zambia (Liverpool John Moores University 2017).

Phiri S, Zambia Digital Rights Landscape Report in Digital Rights in Closing Civic Space: Lessons from Ten African Countries (2021).

Powell A, Data Trust and Accountability in the UK's Information Commissioner's Office (London School of Economics 2020).

Reventlow NJ, Protecting Privacy in the Age of Surveillance (Digital Freedom Fund 2021).

Sukhai NB, 'Hacking and Cybercrime' (8 October 2004) Proceedings of the 1st Annual Conference on Information Security Curriculum Development (ACM, New York).

Wipul Jayawickrama, 'Cyber Crime Threats, Trends and Challenges' (Computer Security Week 2008, Info Shield 2008).

International Instrument

African Union. (2014). African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention). Malabo, Equatorial Guinea.

INTERNET SOURCES

GeeksforGeeks "What is Cyber Security?", explaining the tools and purpose of cybersecurity https://www.geeksforgeeks.org/ethical-hacking/what-is-cyber-security

IBM "What is cybersecurity?" offering clear definitions of systems, people, and data protection. https://www.ibm.com/think/topics/cybersecurity

ScienceNewsToday "Cybersecurity Is a Human Right" describing our digital skeleton and dignity

https://dsisecurity.com/2021/08/09/the-importance-of-cybersecurity-in-todays-society (Accessed on 14/08/2025)

IBM "What is cybersecurity?" offering clear definitions of systems, people, and data protection. https://www.ibm.com/think/topics/cybersecurity

ScienceNewsToday "Cybersecurity Is a Human Right" describing our digital skeleton and dignity Cybersecurity Explained: The Basics of Protecting Your Digital Life

Kemper, Grayson (2019-08-01). "Improving employees' cyber security awareness". *Computer Fraud & Security*. **2019**

GeeksforGeeks “What is Cyber Security?”, explaining the tools and purpose of cybersecurity https://www.geeksforgeeks.org/ethical-hacking/what-is-cyber-security

Global Initiative Against Transnational Organized Crime. Definition of cyber-dependent & impact on data. https://globalinitiative.net/wp-content/uploads/2019/03/TGIATOC-Report-Cybercrime-in-the-UN-01Mar1510-Web.pdf

Security Law blog. Anonymity, IoT, and cybercrime growth factors. https://www.security.law/post/cybercrime-growth-is-unstoppable-and-these-are-the-reasons-why

https://www.cyberdefensemagazine.com/the-true-cost-of-cybercrime-why-global-damages-could-reach-1-2-1-5-trillion-by-end-of-year-2025 (Accessed on 14/08/2025)

https://www.bdemerson.com/article/complete-cybercrime-statistics? (Accessed on 14/08/2025)

INTERPOL. Economic impact of cybercrime. https://www.interpol.int/en/Crimes/Cybercrime? (Accessed on 14/08/2025)

United Nations Office on Drugs and Crime (UNODC). (2024). *United Nations Convention against Cybercrime*. Retrieved from https://www.unodc.org/unodc/en/cybercrime/convention/home.html

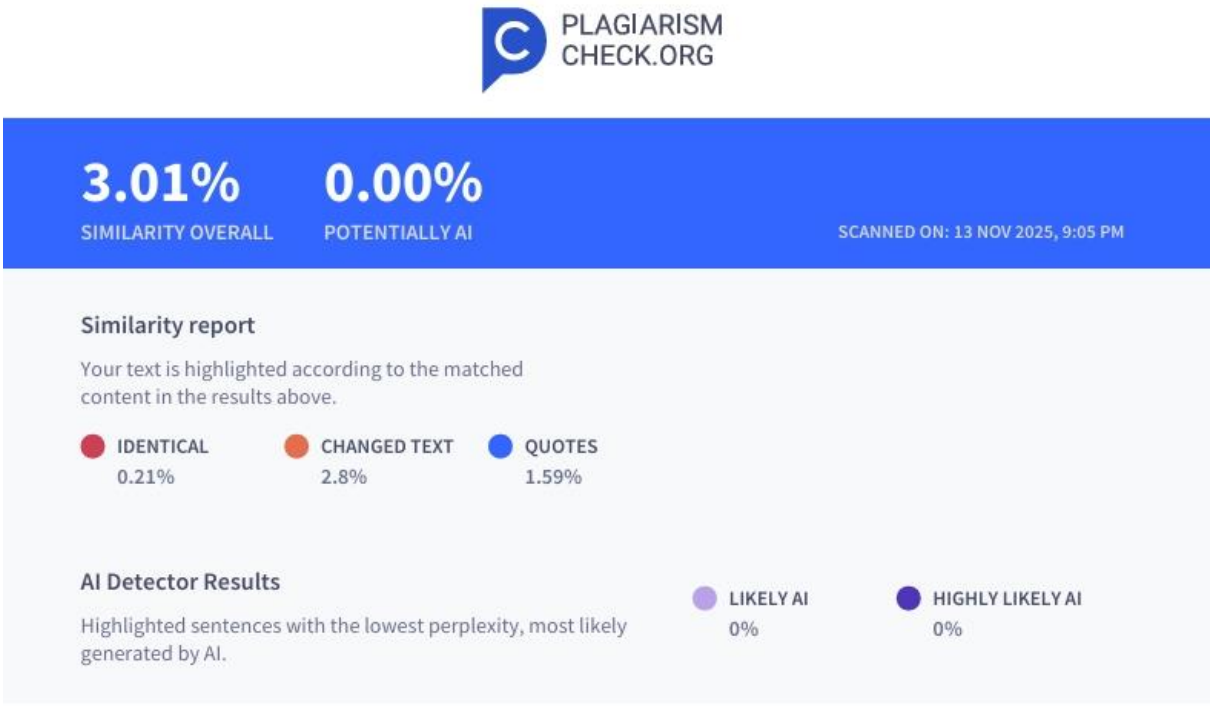
Understanding Data Protection and Privacy Laws in Zambia https://generisonline.com/understanding-data-protection-and-privacy-laws-in-zambia (Accessed on 20/04/2025)

https://www.dataprivacy.academy/post/what-is-data-privacy (accessed on 13/04/2025)

https://www.nadpa-rapdp.org/en/node/220 (accessed on 13/04/2025)

ZAMBIA - Enforcement of the Data Protection Act No. 3 of 2021 Begins in March 2025https://www.nadpa-rapdp.org/en/node/220 (accessed on 13/04/2025)

https://securiti.ai/solutions/zambia-data-protection-act (accessed on 13/04/2025)



Report #29958573

1 2 3 4 5 6 7 8 9 10 A COMPARATIVE ANALYSIS OF ENFORCEMENT - RELATED PROVISIONS IN THE DATA PROTECTION ACT IN ZAMBIA WITH THOSE IN COUNTERPART LEGISLATION IN SOUTH AFRICA KENYA NIGERIA AND THE UNITED KINGDOM SCHOOL OF LAW BY MARGARET BANDA LLB22114013 An obligatory essay submitted to the University of Lusaka in partial fulfillment of the requirement for the award of the Bachelor of Laws (LLB) Degree 2025 i DECLARATION I MARGARET BANDA do declare that this dissertation titled 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 "A COMPARATIVE ANALYSIS OF ENFORCEMENT-RELATED PROVISIONS IN THE DATA PROTECTION ACT IN ZAMBIA WITH THOSE IN COUNTERPART LEGISLATION IN SOUTH AFRICA KENYA NIGERIA AND THE UNITED KINGDOM" 1 2 3 4 5 6 7 8 9 10 which is hereby submitted to the School of Law at the University of Lusaka as part of the requirements for the award of the Bachelor of Laws (LLB) degree is my original work and has not previously been submitted for the award of a degree at this or any other tertiary institution. 1 2 3 4 5 6 7 9 The sources that have been used or quoted have been indicated and duly acknowledged as complete reference Signature…….. 1 2 3 4 5 6 7 8 9 Date ……14/11/2025…….. ii SUPERVISOR'S RE COMMENDATION I,……., do recommend that this dissertation titled 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 21 " A COMPARATIVE ANALYSIS OF ENFORCEMEN T - RELATED PROVISIONS IN THE DATA PROTECTION ACT IN ZAMBIA WITH

UNIVERSITY of LUSAKA

SCHOOL OF LAW

L400B / Dissertation II – DIRECTED RESEARCH (OBLIGATORY ESSAY)

RESEARCH CLEARANCE FORM

NAME: Margaret Banda **STUDENT NUMBER:** LLB22114013

SUPERVISOR: Katongo Chilesha **TOPIC:** A COMPARATIVE ANALYSIS OF ENFORCEMENT-RELATED PROVISIONS IN THE DATA PROTECTION ACT IN ZAMBIA WITH THOSE IN COUNTERPART LEGISLATION IN SOUTH AFRICA, KENYA, NIGERIA AND THE UNITED KINGDOM

Stage	Supervisor's Comments	Supervisor's Signature & Date	Student's Signature & Date
Research Proposal	Proceed to begin Research	[signature]	[signature] 18/04/25
Chapter 1 – Introduction	Proceed with Corrections	[signature]	27/07/25 [signature]
Chapter 2 –	Submit as guided	[signature]	[signature] 15/08/25
Chapter 3 –	Proceed as submitted	[signature]	5/09/25 [signature]
Chapter 4 –	Proceed to Chapter 5	[signature]	11/10/25 [signature]

Chapter 5 – Conclusions & Recommendations	Proceed	[illegible]	23/10/25
Abstract, Table of Contents, Bibliography and Appendices	done. proceed to compile resea	[illegible]	28/10/25
First Draft	Done.	[illegible]	31/10/25
Second Draft	Done.	[illegible]	7/11/25
Final Draft	Ready for submission	[illegible]	14/11/25

Please attach this form to the back of your dissertation at the end of the research, before submission via the Moodle e-learning platform.