EXAMINATION OF LEGISLATIVE FRAMEWORK ON PERSONAL USER DATA IN KENYA: PROMOTION AND PROTECTION OF THE RIGHT TO PRIVACY

Submitted in partial fulfilment of the requirements of the Bachelor of Laws Degree, Strathmore University Law School

By

OMONDI RICHARD ACHIENG

146314

Prepared under the supervision of

Dr. Josephat Kilonzo

Word count (10,701)

April 2025

DECLARATION

I, Omondi Richard Achieng of admission number 146314, do declare that the research proposal titled "Examination of the legislative framework on personal user data in Kenya: promotion and protection of the right to privacy " is the result of my own work and that it has not been submitted for any other academic award. The content of this research proposal is entirely original, except where due reference is made, and the work has been conducted under the supervision of.

I further declare that any assistance I received in preparing this proposal and all sources of materials used in the research have been acknowledged in the proposal. All ethical considerations and guidelines, as set forth by the academic institution of Strathmore University have been adhered to during the preparation and conduct of this research proposal.

I understand the consequences of academic dishonesty, including plagiarism and fabrication of data, and I affirm that this research proposal represents an honest and genuine effort on my part. Any contributions by others to this work have been duly acknowledged.

Signed …

Dated…… 10th April 2025…

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

Signed:..... Date: 10 April 2025

DR. JOSEPHAT KILONZO.

List of Abbreviations

- AG - Attorney General
- CAK - Communications Authority of Kenya
- DPC - Data Protection Commissioner
- ODPC - Office of the Data Protection Commissioner
- COPPA - Children's Online Privacy Protection Act
- DPA - Data Protection Act
- GDPR - General Data Protection Regulation
- KICA - Kenya Information and Communications Act
- POPIA - Protection of Personal Information Act
- CPA - Cybersecurity Protection Act
- DMS - Device Management System
- ICT - Information and Communications Technology
- NIS - National Intelligence Service
- EAC - East African Community
- SASSA - South African Social Security Agency
- UDHR - Universal Declaration of Human Rights
- UN - United Nations

List of Legal Instruments

- The Constitution of Kenya 2010.
- The Kenya Data Protection Act 2019.
- The Consumer Protection Act 2012.
- The Computer Misuse and Cybercrimes Act 2018.
- Protection Of Personal Information Act 2013.
- General Data Protection Regulation (EU) 2016/679.
- Universal Declaration of Human Rights, 1948

List of cases

1. *Lloyd v Google LLC* [2021] UKSC 50.
2. *Australian Competition and Consumer Commission v Google LLC* [2021] HCA 30.
3. *Warren v DSG Retail Ltd* [2021] EWHC 2168 (QB).
4. *Hájovský v. Slovakia* [2021] ECHR.
5. *ES v Shillington* [2021] ABQB 303.
6. *Bloggers Association of Kenya v Attorney General* [2020] eKLR.
7. *Kenya Human Rights Commission v Communications Authority of Kenya* [2018] eKLR.
8. *MWK v Attorney General* [2020] eKLR.
9. *Nubian Rights Forum & Others v Attorney General & Others* [2020] eKLR.
10. *Okiya Omtatah Okoiti v Communications Authority of Kenya & Others* [2018] eKLR.
11. *Bharat Thakrar v WPP Scangroup PLC* [2021] ODPC.
12. *Black Sash Trust v Minister of Social Development & Others* [2017] ZACC 8.
13. *Amabhungane Centre for Investigative Journalism NPC & Another v Minister of Justice & Others* [2021] ZACC 3.

ABSTRACT

Concerns over cybersecurity threats have been raised by Kenya's increasing reliance on digital technology, which has resulted in a rise in the sharing and storing of personal user data. In order to determine the degree to which existing laws protect people's privacy and security on digital platforms, this study analyses Kenya's cybersecurity legal framework with regard to the protection of personal data. It examines current laws that regulate the gathering, storing, and processing of data by public and commercial organisations, with an emphasis on how well enforcement tools and sanctions work to discourage violations.

In order to handle new cybersecurity issues, the study aims to pinpoint the legal framework's flaws and inadequacies and suggest the necessary changes. To identify best practices and lessons that apply to Kenya, a comparison study with countries that have effectively enacted strong cybersecurity laws will be carried out. The study intends to aid in the creation of a more successful legislative and regulatory strategy for safeguarding personal user data in Kenya by pointing out areas that require improvement.

The research is doctrinal in nature and it relies on a desktop approach based on primary and secondary sources. The primary sources include the Constitution, legislation, and regulations. Secondary sources include books, book chapters, and journal articles. The study also relies on a comparative study on South Africa. Among the considerations of this study are comprehensive evaluations of the benefits and drawbacks of the current legislation, recommendations for legislative modifications, and potential impacts of these changes on enhancing the protection of personal user data in Kenya.

In conclusion, this research paper seeks to contribute to the ongoing discussion on cybersecurity laws in Kenya by focusing specifically on the protection of personal user data. The goal of the study is to provide policymakers, attorneys, and other stakeholders with important insights on the legal aspects of data security and privacy. By doing this, they will be able to fortify the current system and ensure that user data is effectively protected in the digital age.

CHAPTER 1: INTRODUCTION

1.1 Background

In today's digital era, the protection of personal user data has become a pressing issue globally. With the rapid advancements in technology and the increasing reliance on digital platforms, the need for robust cybersecurity legislation has become paramount. This research proposal aims to delve into the topic of cybersecurity legislation specifically concerning personal user data in Kenya.

Kenya's data protection framework is primarily governed by the Data Protection Act, 2019, which came into effect on November 25, 2019. This Act operationalizes the right to privacy as outlined in Article 31 of the Constitution of Kenya, 2010[1], specifically clauses (c) and (d) that protect individuals from arbitrary interference with their privacy, family, home, or correspondence. The Act establishes the Office of the Data Protection Commissioner (DPC), which is responsible for overseeing compliance and enforcement of data protection regulations.

Significant loopholes still exist in Kenya's data protection laws' implementation and enforcement, notwithstanding its legislative requirements. The efficacy of the Data Protection Act is hampered by issues including insufficient enforcement measures, low public awareness, and poor institutional capacity[2]. Concerns over the effectiveness of the current legal framework in safeguarding personal user data are also raised by the growing number of instances of data breaches, unauthorised data sharing, and surveillance tactics by both state and non-state actors[3].

Concerns over the efficacy of the current legislative framework in protecting personal user data have also increased due to the rise in cybercrimes, data breaches, and digital surveillance practices—both by government and private organisations. Significant concerns on how to strike a balance between security considerations and the defence of fundamental rights are brought up by

[1] Constitution of Kenya 2010, Article 31.

[2] Data Protection Act, No. 24 of 2019 (Kenya).

[3] Kenya National Commission on Human Rights, 'Data Protection in Kenya: Challenges and Opportunities' (2022).

state-led digital surveillance, excessive data retention by corporations, and unauthorised data access by third parties[4].

The case of *Okoiti v. Communications Authority of Kenya & Another*[5] serves as a landmark ruling affirming the right to privacy in Kenya. The High Court held that the installation of a device management system by the Communications Authority without adequate data protection safeguards violated the constitutional right to privacy. This first highlighted the need and necessity of privacy protection laws and legislation.

The main topic of this study is Kenya's legal framework for protecting personal user data, with an emphasis on how well it upholds and advances the right to privacy. In order to suggest changes that would strengthen Kenya's protection of personal data, it also looks at enforcement issues and draws lessons from similar countries[6], in this research, the chosen jurisdiction is South Africa.

1.2 Statement Of The Problem

The safety of personal user data has become a crucial concern due to Kenya's rapid technological improvement and growing reliance on digital platforms; nevertheless, the efficacy of current solutions is undermined by considerable challenges. The influence of the Data Protection Act of 2019 is limited by enforcement gaps, budget limitations, and poor public awareness, despite the act's goal of operationalising the constitutional right to privacy. The Office of the Data Protection Commissioner (DPC) faces operating difficulties, and organisations are at risk of cybercrime and data breaches due to unclear legal provisions and low compliance. Furthermore, the issue is made worse by the absence of strong procedures to deal with new cybersecurity risks, putting private and public sectors' personal information at danger. This study aims to examine the adequacy of Kenya's legislation on personal user data in Kenya in respect to the promotion and protection of the right to privacy.

---

[4] S. Mutunga, 'The Impact of Digital Surveillance on Privacy Rights in Kenya' (2023) 12 East African Law Journal 89.

[5] *Okoiti v. Communications Authority of Kenya & Another, 2017, eKLR.*

[6] A. Ndung'u, 'Enhancing Data Protection in Kenya: Lessons from South Africa' (2023) 15 East African Law Review 67

1.3 Statement of objectives

Below are the research objectives that guide the study:

i) Examining Kenya's legal framework on personal data protection;

ii) Examining challenges and gaps on collection and use of personal data and implication on privacy; and

iii) Analysing the lessons that Kenya can learn from South Africa on privacy and personal data protection.

1.4 Research Questions

Below are the research questions that guide the study:

1. To what extent does the legal framework ensure data protection?
2. What are the challenges faced in collection and use of personal user data privacy and protection?
3. What lessons can Kenya learn from South Africa?

1.5 Hypothesis

The hypothesis adopted in this research is that Kenyan laws regulating use of personal user data are not sufficient to prompt nor protect the right to privacy and need to be revised in order to cater for all the provisions of personal user data protection.

1.6 Significance of the study

The right to privacy is a fundamental human right, enshrined in various international and regional instruments. Article 12 of the Universal Declaration of Human Rights (UDHR) provides that no one shall be subjected to arbitrary interference with their privacy, family, home, or correspondence[7]. The right to privacy and protection from unauthorised intrusion are also guaranteed by Article 17 of the International Covenant on Civil and Political Rights (ICCPR)[8]. The right to dignity, which is inextricably related to privacy, is likewise recognised under the African Charter on Human and Peoples' Rights (ACHPR)[9].

[7] Universal Declaration of Human Rights, UNGA Res 217 A (III) (10 December 1948), art 12.

[8] International Covenant on Civil and Political Rights, UNGA Res 2200A (XXI) (16 December 1966), art 17.

[9] African Charter on Human and Peoples' Rights, OAU Doc CAB/LEG/67/3 rev 5 (21 October 1986), art 5.

At the national level, the right to privacy is specifically protected by Article 31 of the Kenyan Constitution[10], which protects people from needless monitoring, improper use of data, and illegal access to personal data. Furthermore, by creating a legislative framework for the control of the processing of personal data, the Data Protection Act, 2019 was passed in order to operationalise this right[11]. Nevertheless, the effective realisation of the right to privacy is nevertheless hampered by enforcement issues, noncompliance, and low public awareness, even in the face of these legislative safeguards. These issues are highlighted in the *Okoiti v. Communication Authority of Kenya & Others*[12] case, which highlights the necessity of a strong data protection system that is both legally recognised and successfully applied in real-world situations. The research seeks to benefit individuals within the Kenyan jurisdiction that use internet enabled devices and store their personal information on the internet and share the data with different websites and online enterprises.

Examining Kenya's legal framework regarding personal user data is crucial in order to determine if it adequately upholds and advances the right to privacy. The law needs to keep up with new dangers to the protection of personal data since digital technology and data-driven enterprises are developing so quickly. In *Packer v. Packer*[13], Lord Denning famously said, "The law must keep pace with the times." In order to make sure Kenya's data protection laws are efficient, thorough, and in line with international best practices, this study aims to identify legislative loopholes, assess enforcement mechanisms, and make recommendations for strengthening them.

1.7 Theoretical Framework

1. Privacy Theory:

Theory of privacy, such as those proposed by Alan Westin and Daniel Solove, can provide a foundational understanding of the concept of privacy[14], its dimensions, and its importance in the

[10] Constitution of Kenya (2010), art 31.

[11] Data Protection Act, No 24 of 2019 (Kenya).

[12] *Okoiti v. Communication Authority of Kenya & Others, 2017, eKLR.*

[13] Packer v Packer, 1954, EWCA Civ 1.

[14] Solove, Understanding Privacy, 1 ed, Harvard University Press, Massachusetts, 2010, 248.

digital age. These theories can help conceptualize the need for personal data protection and the potential risks and consequences of privacy violations in the context of cyber security.The theories of privacy articulated by Alan Westin and Daniel Solove provide essential frameworks for understanding the complexities of privacy in the context of personal data protection. Alan Westin, in his influential work "Privacy and Freedom" (1967), defined privacy as the right of individuals to control their personal information and to determine when, how, and to what extent that information is communicated to others. He identified four fundamental states of privacy: solitude, intimacy, anonymity, and reserve. These states reflect different ways individuals seek to manage their interactions with others and maintain their privacy in various social contexts. Westin's work laid the groundwork for modern privacy legislation and highlighted the importance of individual autonomy in the face of growing surveillance technologies and data collection practices.

Daniel Solove expanded on Westin's ideas by proposing a comprehensive taxonomy of privacy that categorizes various privacy issues into distinct types. In his 2006 article "A Taxonomy of Privacy," Solove identified four general categories of privacy problems: information collection, information processing, information dissemination, and invasion. He argued that traditional definitions of privacy often overlook the broader implications of these categories, which can lead to inadequate legal protections for individuals. Solove emphasized that privacy is not merely about secrecy but encompasses a range of concerns related to personal autonomy, dignity, and the social implications of data handling practices. His work underscores the need for a multifaceted approach to privacy that considers both individual rights and societal responsibilities.

In relation to my dissertation these theories are instrumental in framing my analysis of how Kenyan legislation addresses privacy concerns in the digital age. By applying Westin's concept of privacy as control over personal information, I can evaluate whether current laws empower individuals to manage their data effectively. Furthermore, Solove's taxonomy allows me to dissect specific privacy challenges faced by users in Kenya, such as issues related to data collection by both private companies and government entities. This theoretical framework facilitates a deeper understanding of the effectiveness of existing cyber security legislation in promoting and protecting the right to privacy within Kenya's evolving digital landscape.

1.8 Literature Review

Ethical considerations are crucial in this context. Helen Nissenbaum, in her book "Privacy in Context: Technology, Policy, and the Integrity of Social Life,"[15] explores the ethical dimensions of personal data collection and the importance of user control. Her studies delve into the ethical responsibilities of companies in handling user data, emphasizing the need for transparency, fairness, and accountability.

The concept of informed consent is often discussed regarding wearable device data. Alan Westin, in his book "Privacy and Freedom,"[16] emphasizes the need for individuals to have informed control over their personal information. He majors on the complexity of informed consent due to data collection practices by companies. Examining the types and purposes of data collected by wearable devices is crucial for assessing privacy implications. His study analyzes the data collection practices of popular wearable devices, emphasizing the need for transparency and informed consent.

Kate Crawford, in her work "The Hidden Biases in Big Data,"[17] examine the potential biases and discrimination that can arise from the collection and use of personal data from internet enabled devices. The study explores scenarios where data-driven decisions may infringe upon users' autonomy and underscore the importance of ethical considerations in the development and deployment of wearable technologies.

Ryan Calo, in his book "The Law of Robots,"[18] discusses the legal implications of technology and the rights of individuals to control their personal data. He does analyze existing data protection laws and their applicability to technology. He then provides a comparative analysis of international regulations, highlighting gaps and challenges in safeguarding user rights.

[15] Nissenbaum, Privacy in Context, 1 ed, Stanford University Press, Stanford, 2009, 56.
[16] Westin, Privacy and Freedom, 1 ed, Ig Publishing, Columbia, 2015, 309.
[17] Crawford, The Hidden Biases in Big Data, 1 ed, Harvard Business Publishing, Massachusetts, 2013, 34.
[18] Calo, The Law of Robots, 1 ed, Stanford University Press, Stanford, 2016, 104.

Helen Nissenbaum's work, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, offers an essential theoretical framework for understanding privacy as a contextual and relational issue. Nissenbaum argues that the ethical collection of personal data requires a nuanced understanding of context, particularly the rights of users to control their data and to be informed of how it is used. Nissenbaum's concept of "contextual integrity" stresses the importance of aligning data practices with societal norms and expectations[19]. This concept resonates with the ethical challenges that companies and governments face globally, including in Kenya, as they navigate the intersection of data collection, privacy, and security.

Researchers and legal professionals have vigorously debated the scope and limitations of privacy rights in Kenya.

Willy Mutunga's article "Constitutionalism and Digital Privacy in Kenya", his study shows how data protection vulnerabilities, particularly in the areas of biometric data collection and monitoring, have been exposed by Kenya's digital transformation[20], thus pointing out a need for comprehensive legislative protection. Nicholas Kibet and Peter Ouma's "Data Privacy in Kenya: Challenges and Prospects". The authors point out that government agencies regularly abuse their vast monitoring powers to circumvent privacy laws, criticising the Data Protection Act's enforcement limitations[21], hereby highlighting the misuse of government bodies on intruding on unauthorised personal user data.

In "Cybersecurity and Privacy in Africa", John Odhiambo contrasts the data protection regulations of Kenya and South Africa's POPIA with global standards like the GDPR[22] ; John Odhiambo compares the data protection laws of South Africa and Kenya in his book "Cybersecurity and Privacy in Africa". He focusses on the Protection of Personal Information Act (POPIA), 2013 and the Data Protection Act, 2019 in Kenya. He highlights the main parallels and divergences between domestic frameworks and international norms like the General Data Protection Regulation

[19] Nissenbaum, Privacy in Context, 1 ed, Stanford Law Books, California, 2009, 270.

[20] Willy Mutunga, *Constitutionalism and Digital Privacy in Kenya* (Nairobi: Strathmore University Press, 2021) 45.

[21] Nicholas Kibet & Peter Ouma, *Data Privacy in Kenya: Challenges and Prospects* (Nairobi: University of Nairobi Law Journal, 2022) 67.

[22] John Odhiambo, *Cybersecurity and Privacy in Africa* (Cape Town: Juta Law Publishers, 2020) 89.

(GDPR) of the European Union in terms of its reach, methods of enforcement, and efficacy in protecting personal information. Odhiambo talks on how South Africa and Kenya have addressed regional issues particular to the African regulatory environment while also incorporating elements of international best practices, such as accountability, data minimisation, and consent. His analysis clarifies each legislative framework's advantages and disadvantages in terms of ensuring strong cybersecurity and data protection in the digital era.

This dissertation seeks to bridge these gaps by critically examining the effectiveness of Kenya's cybersecurity legislation, particularly the **Data Protection Act, 2019**, in promoting and protecting privacy rights. It assesses the extent to which Kenya's data protection framework aligns with international standards and the practical challenges of enforcing these protections.

1.9 Research Methodology

This study adopts doctrinal research methodology. It relies on a desktop approach based on primary and secondary sources. The primary sources include the Constitution, legislation, and regulations. Secondary sources include books, book chapters, and journal articles. The study also relies on a comparative study on South Africa. This is because Kenya can borrow some lessons from South Africa which has progressive legislation and judicial decisions which enhance privacy in the use of personal data.

1.10 Limitations of the study

When researching "Cyber Security Legislation on Personal User Data in Kenya," several limitations should be considered. These include the limited availability of up-to-date data on cybersecurity incidents[23], personal data breaches [24] and the implementation of laws, as well as restricted access to government reports or industry statistics.

[23] Roebuck, Data Breach Notification Laws, 1ed, Emereo PTY Limited, Queensland, 2011, 317.

[24] Shoniregun, Impacts and Risk Assessment of Technology for Internet Security, Springer US, Connecticut, 2005, 97.

1.11 Chapter Breakdown

Chapter 1 gives a brief overview of the research paper. It introduces the problem and outlines the objectives the paper seeks to fulfil by the end of the study. It provides the theory the paper is based on and gives insight on the literature to be used in the paper. It concludes by giving a breakdown of the chapters the paper expounds on.

Chapter 2 focuses on the legal framework governing personal user data in Kenya. It begins with examining the Constitution of Kenya, then proceeds to the Data Protection Act and the measures enshrined within these legislations together with the problems they are geared to solve.

Chapter 3 is on the challenges and the gaps that undermine the effectiveness of Kenya's legal framework in regards to personal user data privacy and protection.

Chapter 4 provides a comparison of Kenya's regulations regarding individual user data and cyber security to South Africa's. It is feasible to pinpoint prospective best practices and areas in which Kenya's cybersecurity ecosystem needs to be improved by contrasting it with those of other countries.

Chapter 5 concludes the research. It offers recommendations concerning the legal framework regarding laws on personal data privacy and protection in Kenya.

CHAPTER 2: LEGAL FRAMEWORK GOVERNING PERSONAL USER DATA IN KENYA

2.1 Introduction

One essential component of Kenyans' right to privacy is the protection of their personal user data. The legal framework governing the protection of personal user data in Kenya is examined in this chapter, starting with constitutional principles and moving on to statutory laws like the Data Protection Act (DPA), 2019 and its implementing regulations. The chapter also examines pertinent case law and judicial interpretations of personal data protection laws and the right to privacy

2.2 Constitutional Protection of the Right to Privacy

Everybody is guaranteed the following rights and protections under Article 31 of the 2010 Kenyan Constitution: Primarily, it gives that a person is granted the right not to have their person, home, or property searched; secondly to have information about their private affairs or family not required or disclosed without a warrant; and most importantly and relevant to this research paper, not to have the privacy of their communications violated[25].

Courts have played a significant role in determining the scope of Article 31 in a number of situations. This article is elaborated in the case of *Nairobi Law Monthly Company Limited v Kenya Electricity Generating Company & 2 others*[26] where the court gave the scope and limitations of the right to privacy. This provision lays the foundation for Kenya's data protection laws and practices by guaranteeing that private data is shielded from unlawful access, acquisition, and use.

The High Court held in *Okiya Omtatah Okoiti v. Communication Authority of Kenya & 8 Others* [2018] that the government's plan to implement a Device Management System (DMS) in mobile networks that might access private conversations violated Article 31 of the Constitution[27]. The decision underlined that any restriction on privacy must pass the reasonableness and necessity standards set forth in the constitution.

[25] Constitution of Kenya, 2010, Art. 31.

[26] *Nairobi Law Monthly Company Limited v Kenya Electricity Generating Company & 2 others, 2013, eKLR.*

[27] Okiya Omtatah Okoiti v Communication Authority of Kenya & 8 Others [2018] eKLR.

In a similar vein, the court in *Katiba Institute v. President of Kenya & Others* [2020] determined that robust data protection measures were required to stop misuse of the personal data gathered and stored under the Huduma Namba program, highlighting the importance of safeguarding privacy in digital identification systems[28]. The court determined that robust privacy safeguards must be in place while collecting and preserving personal data in order to prevent misuse. The decision underlined the need of transparency, accountability, and public participation in digital identity programs.

Kenyan courts and the ODPC have increasingly played a role in interpreting the Data Protection Act and its application to various sectors. In *Bharat Thakrar v WPP Scangroup PLC [2021]*The ODPC's discovery of a corporation that had inappropriately managed personal information in violation of data protection regulations underscored the importance of DPA compliance[29].

In *Kenya Human Rights Commission v Communications Authority of Kenya [2022]* **a**ccording to the Court, government agencies are required to abide by data protection regulations, which include obtaining the appropriate consent before processing personal data[30].

In the *Nairobi Law Monthly v. Kenya Electricity Generating Company (KenGen) [2013*][31], the court considered whether it was feasible to compel a public entity to provide information that contained personal data. It concluded that while if the right to access information is guaranteed by Article 35, this right must be balanced against the privacy protections offered by Article 31.

Benard Murage v. Fineserve Africa Limited & 3 Others [2015][32], the unconsented sharing of mobile subscriber data with external advertising was questioned by the petitioner. The court reaffirmed that companies must get user consent before processing personal data in compliance with international data protection laws like the General Data Protection Regulation (GDPR).

[28] Katiba Institute v President of Kenya & Others [2020] eKLR.

[29] Bharat Thakrar v WPP Scangroup PLC [2021] ODPC Decision.

[30] Kenya Human Rights Commission v Communications Authority of Kenya [2022] eKLR.

[31] Nairobi Law Monthly v. Kenya Electricity Generating Company (KenGen) [2013 eKLR.

[32] Benard Murage v. Fineserve Africa Limited & 3 Others [2015] eKLR.

2.3 The Data Protection Act, 2019

The Data Protection Act, 2019 (DPA) is Kenya's primary law governing the protection of personal information. It was approved to operationalise Article 31 of the Constitution and bring Kenya's legal system into line with best practices from across the world. The Act establishes guidelines, rights, and obligations related to the gathering, processing, and storing of data.

2.4 Key Provisions of the DPA

The DPA outlines fundamental data protection principles, including: Lawfulness, fairness, and transparency; Personal data must be processed in a lawful and transparent manner[33]. Personal data must be processed in accordance with the law, meaning organizations must have a valid legal basis for collecting and using it. This could include user consent, contractual necessity, legal obligation, public interest, or legitimate interest. Additionally, processing must be fair, ensuring that individuals are not misled or harmed, and transparent, meaning that data subjects should be informed about how their data is being used.

Purpose limitation; Data should only be collected for specified, explicit, and legitimate purposes[34]. Organizations must collect personal data only for specific, explicit, and legitimate purposes. This prevents the indiscriminate collection of data and ensures that it is not used for secondary purposes beyond what was originally stated without obtaining further consent from the data subject. Data minimization; Organizations must only collect data necessary for the intended purpose[35]. Only the minimum amount of personal data necessary to achieve the intended purpose should be collected and processed. This principle discourages excessive data collection, reducing risks such as unauthorized access, misuse, and data breaches. Storage limitation; Personal data should not be retained longer than necessary[36]. Personal data should not be retained for longer than necessary. Organizations must establish data retention policies to determine how long personal data is needed and implement secure deletion or anonymization methods once the retention period expires. Accountability; Data controllers and processors are responsible for ensuring compliance with the

[33] Data Protection Act, No. 24 of 2019 (Kenya), s 25.

[34] Data Protection Act, No. 24 of 2019 (Kenya), s 26.

[35] Data Protection Act, No. 24 of 2019 (Kenya), s 27.

[36] Data Protection Act, No. 24 of 2019 (Kenya), s 28.

DPA[37]. Data controllers (entities that determine the purpose and means of processing personal data) and data processors (entities that process data on behalf of controllers) are responsible for ensuring compliance with the DPA. They must implement appropriate policies, procedures, and security measures and may be required to demonstrate compliance upon request by the regulator.

The Act also establishes the Office of the Data Protection Commissioner (ODPC), tasked with overseeing compliance, investigating complaints, and enforcing penalties for data breaches[38]. It is responsible for: monitoring and enforcement; ensuring that organizations adhere to the DPA's provisions, investigating complaints; handling complaints from individuals regarding data privacy violations, issuing guidelines and directives; providing guidance on best practices for data protection, imposing penalties; enforcing administrative fines and other corrective measures for non-compliance, including data breaches and unlawful data processing.

2.5 Regulations under the Data Protection Act

To implement the DPA effectively, the government has enacted subsidiary regulations, including:

The Computer Use and Cyber Crimes Act 2018: this act criminalizes cyber-related offences. This covers, Unauthorized Access and Interference[39]; It forbids unauthorised password sharing, illegal access to computer systems, and data manipulation that can compromise personal data. Cyber Harassment and Identity Theft[40]; The Act shields people from online abuse, identity theft, and other crimes that might result from improper use of data. Enforcement and Investigative Powers[41]; The Act strengthens the enforcement of data protection rules by giving agencies, such as the National Computer and Cybercrimes Coordination Committee, the ability to look into cybercrimes.

Comprehensive guidelines for the legitimate processing of personal data are provided by the *Data Protection (General) Regulations*, 2021[42]. They mandate that explicit, freely provided, informed

[37] Data Protection Act, No. 24 of 2019 (Kenya), s 30.

[38] Data Protection Act, No. 24 of 2019 (Kenya), s 6.

[39] Computer Misuse and Cyber Crimes Act 2018, s 14.

[40] Computer Misuse and Cyber Crimes Act 2018, s 27.

[41] Computer Misuse and Cyber Crimes Act 2018, s 51-56.

[42] Data Protection (General) Regulations, 2021, Legal Notice No 217 of 2021.

consent be obtained by data controllers and processors; this consent must be particular and revocable at any moment. Data subjects are entitled to access their personal information, ask for data portability, object to processing that violates their privacy, and request that outdated or erroneous information be corrected or deleted. Additionally, the restrictions restrict the amount of time that businesses can keep personal data and mandate that it be securely disposed of when not needed.

All organisations that handle personal data, whether as controllers or processors, are required under the *Data Protection (Registration of Data Controllers and Data Processors) Regulations*, 2021[43], to register with the ODPC. Those that process data for national security, legal proceedings, or personal use are exempt. To guarantee proper control, the ODPC groups registrants according to the amount and sensitivity of data handled. Penalties, registration revocation, or suspension could result from noncompliance.

Failure of an entity's capacity to process personal data may be subject to fines, suspension, or revocation for noncompliance with registration requirements:

The Data Protection (Complaints Handling and Enforcement Procedures) Regulations, 2021 – These regulations set out procedures for lodging complaints and the enforcement mechanisms available to the ODPC[44]; these rules specify how people can file a complaint if their data protection rights are violated, as well as the ODPC's authority to look into complaints, impose fines, and enforce adherence to the Data Protection Act.. Important characteristics are:

Data subjects have the option to file complaints with the ODPC about unlawful data acquisition, abuse, security breaches, or non-adherence to the Data Protection Act[45]. Details of the claimed infraction and any supporting documentation must be included in complaints. Mechanisms for Investigation and Enforcement: The ODPC is empowered to: Look into claims of violations, issue compliance orders that call for remedial measures[46]. For non-compliance, impose administrative

[43] Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021, Legal Notice No 263 of 2021.

[44] Data Protection (Complaints Handling and Enforcement Procedures) Regulations, 2021, reg 5.

[45] The Data Protection (Complaints Handling and Enforcement Procedures) Regulations, 2021, reg. 7(1).

[46] The Data Protection (Complaints Handling and Enforcement Procedures) Regulations, 2021, reg. 9(2).

fines or other sanctions[47]. Alternative Dispute Resolution (ADR): This process promotes the quick and economical settlement of data protection complaints by resolving disagreements in certain situations through mediation or arbitration[48].

2.6 Conclusion

The Article 31 of the Constitution, the Data Protection Act, 2019 (DPA), and its subsidiary regulations, which all provide extensive protections for privacy rights, form the foundation of Kenya's legal framework for protecting personal user data. Fundamental data protection principles including lawfulness, fairness, purpose limitation, and accountability are included into the legal system, guaranteeing the transparent and secure processing of personal data. By highlighting the necessity of protections in data collection, storage, and processing, especially in situations involving government surveillance, biometric data collecting, and digital identity systems, court rulings have further strengthened the constitutional right to privacy. Kenya's strategy demonstrates its dedication to enhancing privacy and data security and is in line with international best practices, especially the General Data Protection Regulation (GDPR).

[47] The Data Protection (Complaints Handling and Enforcement Procedures) Regulations, 2021, reg. 11(1).

[48] The Data Protection (Complaints Handling and Enforcement Procedures) Regulations, 2021, reg. 14(3).

CHAPTER 3: CHALLENGES AND GAPS THAT UNDERMINE EFFECTIVENESS OF KENYA'S LEGAL FRAMEWORK

3.1 Introduction

The protection and advancement of the right to privacy remain pressing concerns in an era of rapid technological advancements. With the exponential growth of digital technologies and the increasing reliance on online platforms for communication, commerce, and governance, safeguarding personal data has become more critical than ever. Kenya has enacted legislative measures such as the Data Protection Act, 2019, to address these challenges and create a robust framework against cyber risks, data breaches, and unauthorized access to personal information[49].

Despite these legal frameworks, several gaps and challenges persist in ensuring data privacy. This chapter examines the difficulties in enforcing Kenya's data protection laws, including inadequate enforcement mechanisms, overlapping legal provisions, and gaps in judicial interpretation.

3.2 Overlapping and Conflicting Legal Provisions

The Computer Misuse and Cybercrimes Act of 2018[50] and the Kenya Information and Communications Act of 1998[51] are two of the several legislations that constitute Kenya's data protection and cybersecurity regime, seeing as there are duplicative responsibilities under these laws, enforcing authorities may face jurisdictional issues, for example, in the regulation of data breaches and cybercrime, the ODPC and the Communications Authority of Kenya (CAK) usually have conflicting mandates as seen in redundant provisions of the law in sections 8 and 9 of the Data Protection Act[52] that conflict with sections 5 and 6[53] of the Computer Misuse and Cybercrimes Act[54].

[49] Karanja, P., *Digital Privacy and Cybersecurity in Kenya*, Nairobi University Press, 2020.

[50] Computer Misuse and Cybercrimes Act, No 5 of 2018

[51] Kenya Information and Communications Act, No. 2 of 1998 (Revised 2013

[52] Data Protection Act 2019, S 8 -9.

[53] Computer Misuse and Cybercrimes Act 2018, S 5-6.

[54] Nyawa S., Regulatory Overlaps in Kenya's Data Protection and Cybersecurity Framework, East African Journal, Vol 5(2), p112-134.

3.3 Lack of Comprehensive Cybersecurity Regulations

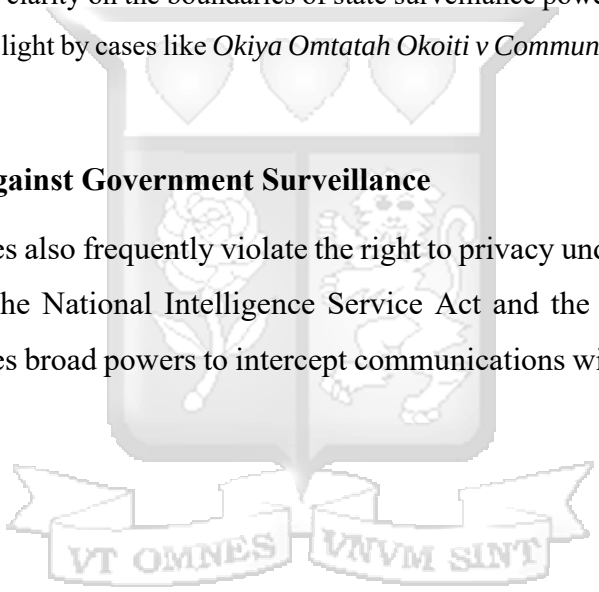
Although it criminalizes cybercrimes like hacking and unauthorized access to information[55], the Computer Misuse and Cybercrimes Act of 2018 fails to specify the necessary cybersecurity legislation regulating government agencies and enterprises[56]. Kenya's regulatory landscape remains dispersed and devoid of explicit technical standards, in contrast to the European Union's General Data Protection Regulation (GDPR), which enforces stringent security requirements[57].

3.4 Inconsistent Judicial Interpretation

Where the meaning of cybersecurity and data protection law is in question, the court has a fundamental role to play. Kenyan courts have not yet established a strong body of case law regarding digital privacy rights[58], though. The lack of judicial clarity on the boundaries of state surveillance powers and the privacy rights of individuals[59] was brought to light by cases like *Okiya Omtatah Okoiti v Communications Authority of Kenya & Others.*

3.5 Weak Protections Against Government Surveillance

State surveillance activities also frequently violate the right to privacy under Article 31 of the 2010 Kenyan Constitution[60]. The National Intelligence Service Act and the Prevention of Terrorism Act[61] give security services broad powers to intercept communications with insufficient protection in place [62].



[55] *Computer Misuse and Cybercrimes Act, s 14.*

[56] Kariuki, J. & Mutunga P., Gaps in Kenya's Cybersecurity Legal Framework: An Analysis of the Computer Misuse and Cybercrimes Act, East African Law Review, Vol. 6(1), p 45-67.

[57] *General Data Protection Regulation (EU) 2016/679.*

[58] *Okiya Omtatah Okoiti v Communications Authority of Kenya & Others [2018] eKLR.*

[59] European Commission, *General Data Protection Regulation: Implementation Guide*, 2020.

[60] Kibet N. & Ouma P. 2022, Data Privacy in Kenya: Challenges and Prospects, Kenya Law Journal, Vol. 8(2), p 112-135.

[61] Prevention of Terrorism Act, No. 30 of 2012, Laws of Kenya.

[62] *National Intelligence Service Act, No. 28 of 2012 (Kenya).*

3.6 Insufficient Public Awareness and Compliance Culture

The majority of Kenyan individuals and entities are not aware of their data protection rights and responsibilities[63]. Due to ignorance, organizations fail to install proper cybersecurity systems[64], and people rarely sue for data breaches because they do not know their rights under the Data Protection Act, 2019[65].

3.7 Absence of Clear Data Breach Notification Requirements

Kenya's Data Protection Act merely imposes broad responsibilities with no explicit deadlines for reporting breaches[66], in contrast to the GDPR, which requires data controllers to inform impacted persons and regulators in the event of a data breach[67]. As a result, consumer protection procedures are weakened and compliance becomes unclear[68].

3.8 Limited Cross-Border Data Protection Frameworks

Kenya does not have overall legislation governing cross-border data flows. Cross-border data transfers are, however, governed by the Data Protection Act of 2019[69], but there is no clear enforcement structure to guarantee conformity[70]. Multinationals and cloud computing service providers operating in Kenya risk processing information inappropriately because of this discrepancy[71].

3.9 Challenges in Enforcement

Inadequate Enforcement Mechanisms

With the establishment of the Office of the Data Protection Commissioner (ODPC) under the Data Protection Act of 2019, enforcement is still lacking despite this, owing to a funding and technical

---

[63] *Office of the Data Protection Commissioner Annual Report (2022).*

[64] Odhiambo, J., *Public Awareness in Digital Privacy*, Journal of East African Law, 2021.

[65] *Data Protection Act, s 25.*

[66] ICT Authority, *Kenya Cybersecurity Report*, 2023.

[67] *GDPR, Art. 33.*

[68] *Data Protection Act, s 43.*

[69] *Data Protection Act, s 48.*

[70] United Nations Economic Commission for Africa, *Cross-Border Data Regulation in Africa*, 2021.

[71] Data Protection Act Kenya 2019, s 25.

deficiency; the ODPC lacks in manpower and substandard technology to effectively monitor and prosecute data infringement[72]. As realized through instances where private organizations utilize or divulge information about users at whim without serious legal repercussions[73], this has created inadequate security for personal information[74].

The crossing of borders by data introduces yet another level of complication[75]. International collaboration and legal harmonization are required to resolve the possible discrepancies in privacy standards that data would face across borders[76]. Kenya should work with international organizations and its neighbors in developing uniform and legally binding data protection standards[77]. The United Nations Conference on Trade And Development (UNCTAD) Report on Data Protection highlights the need for regional cooperation in Africa to develop robust data governance framework[78].

3.10 Conclusion

An important element in protecting user data is Kenya's data protection legislative framework, which is mostly based on the Data Protection Act of 2019. The efficacy of the legislation is still undermined by a number of loopholes and difficulties that still exist in spite of these legal developments. While the lack of comprehensive cybersecurity rules exposes organisations to data breaches, the existence of overlapping and contradictory legal obligations, such as the mandates of the ODPC and CAK, makes enforcement difficult. Furthermore, legal certainty is further complicated by the absence of a well-developed corpus of judicial interpretation on cybersecurity and privacy legislation, which makes it challenging to provide clear precedents for new digital risks.[79]. Furthermore, the practical implementation of data privacy rights in Kenya is still hampered by difficulties with enforcement, inadequate safeguards against governmental monitoring, and low public awareness. The ODPC's lack of enough resources makes compliance problems worse, and

[72] Office of the Data Protection Commissioner (ODPC), *Annual Report 2022*.

[73] Kibwana, M., *Challenges in Data Security: A Kenyan Perspective*, East African Journal of Law, 2021.

[74] *Bharat Thakrar v WPP Scangroup PLC [2021] ODPC Decision.*

[75] World Bank, *Data Governance in Africa*, 2022.

[76] United Nations Economic Commission for Africa, *Cross-Border Data Regulation in Africa*, 2021.

[77] International Cybersecurity Review, vol. 12, no. 3 (2020): 200-223.

[78] United Nations Conference on Trade and Development (UNCTAD), *Data Protection Trends in Africa*, 2023.

[79] Shared Responsibility in Data Privacy, Nairobi: Policy Brief, 2020, p. 16.

the absence of well-defined cross-border data protection procedures leaves international corporations doing business in the nation with legal difficulties. Kenya must improve public understanding of data privacy rights, connect its legal system with global best practices, and fortify enforcement agencies in order to meet these issues. The current legal system will find it difficult to offer the strong protection that Article 31 of the 2010 Constitution calls for in the absence of such revisions.

CHAPTER 4: WHAT LESSONS CAN KENYA BORROW FROM SOUTH AFRICA?

4.1 Introduction

Numerous national, regional, and international legal systems recognize the right to privacy as a basic human right. Strong legal frameworks are necessary to protect personal information from unauthorized access, abuse, or monitoring in the digital age, when data is a major driver of social and economic activity. Through the Constitution, the Protection of Personal Information Act (POPIA), and other ancillary laws, South Africa has established a thorough legal framework that regulates cybersecurity and data privacy. Kenya is still improving its data governance framework after passing the Data Protection Act of 2019. In order to improve its data protection system, Kenya can learn from South Africa's data privacy regulatory framework, which is examined in this chapter along with important court interpretations.

4.2 Constitutional Framework in South Africa

Section 14 of the Constitution of the Republic of South Africa, 1996[80], contains the legal basis for data privacy in South Africa. Every person's right to privacy is guaranteed by this clause, which also protects them from communications interception, seizures, and searches. Especially in the digital age, the courts have been essential in establishing the extent of privacy rights.

The following are cases that speak specifically on the right to privacy and what it means within the South African context; what the South African Constitutional Court has held about Section 14 and the right to privacy;

Bernstein and Others v Bester NO and Others (1996)[81]: The Court recognised the difficulty of defining privacy in this seminal decision, characterising it as "amorphous and elusive." The ruling highlighted that a person's right to privacy is strongest in their most private domain, which includes their home environment, sexual preferences, and family life. But people's expectations of privacy decline as they participate in group activities like social or professional encounters.

[80] Constituion of South Africa 1996, Section 14.

[81] *Bernstein and Others v Bester NO and Others (1996).*

Smuts and Another v Botha (2022)[82]*;* The conflict between the freedom of expression and the right to privacy was discussed by the Supreme Court of Appeal. The Court determined that in this case, the right to freedom of expression superseded the right to privacy since disclosing information about unethical animal trapping activities was in the public interest.

4.3 Legislative Framework

4.3.1 Protection of Personal Information Act (POPIA), 2013

The main law governing the protection of personal data in South Africa is POPIA[83]. By establishing guidelines for the legitimate handling of personal data, it operationalises the fundamental right to privacy. POPIA mandates that before collecting personal data, data controllers and processors must have informed consent, put security measures in place to safeguard the data, and give people the ability to see and update their personal data. The Information Regulator, an independent organisation empowered to enforce compliance, impose penalties, and look into data breaches, is also established under the legislation.

POPIA operationalizes the right to privacy as provided under Section 14 of the Constitution of the Republic of South Africa, 1996[84] that establishes the right to privacy and the scope in which privacy covers. In accordance with POPIA, there is an Information Regulator established with the capability to enforce adherence and issue sanctions for non-adherence[85]. Additionally, the Cybercrimes Act, 2020[86], addresses unauthorized data access, cyber-related fraud, and other offenses.

South Africa's institutional framework for cybersecurity and personal data protection is further reinforced by various entities. The Information Regulator, established under POPIA, is tasked with monitoring and enforcing compliance with data protection laws, handling complaints, and

[82] *Smuts and Another v Botha (2022).*

[83] Protection of Personal Information Act 4 of 2013.

[84] Constitution of the Republic of South Africa, 1996, s 14.

[85] Constitution of the Republic of South Africa, 1996, s 39.

[86] Cybercrimes Act, No. 19 of 2020 (South Africa).

conducting investigations into data breaches. It also collaborates with other law enforcement agencies to ensure proper enforcement of data privacy regulations[87].

The Cybersecurity Hub, under the Department of Communications and Digital Technologies, plays a key role in coordinating national cybersecurity efforts, providing guidelines on best practices, and fostering public-private partnerships to enhance cyber resilience[88]. The State Security Agency (SSA) also contributes through its Cybersecurity Centre, which focuses on national cybersecurity threats, intelligence gathering, and incident response[89]. Additionally, the South African Police Service (SAPS) has specialized cybercrime units that investigate offenses related to unauthorized data access, identity theft, and online fraud[90].

4.3.2 The 2020 Cybercrimes Act

Crimes including identity theft, cyber fraud, illegal communication interception, and unauthorised access to computer systems are all made illegal by the Cybercrimes Act[91]. By guaranteeing that infractions pertaining to data security and cyberthreats are successfully addressed through legal sanctions and law enforcement procedures, it enhances POPIA.

4.3.3 Electronic Communications and Transactions Act (ECTA), 2002

ECTA provides a regulatory framework for digital transactions, including electronic signatures, encryption, and consumer protection in online spaces[92]. It enhances cybersecurity measures by setting standards for electronic communications and protecting personal information in e-commerce transactions. Furthermore, the Electronic Communications and Transactions Act

[87] Cybercrimes Act, No. 19 of 2020 (South Africa), s 50.

[88] Department of Communications and Digital Technologies, *Cybersecurity Hub Overview* (2023) https://www.cybersecurityhub.gov.za accessed [2023].

[89] State Security Agency, *Cybersecurity Centre Mandate* (2023) https://www.ssa.gov.za accessed [2023].

[90] South African Police Service, *Cybercrime Unit Operations* (2023) https://www.saps.gov.za accessed [2023].

[91] Computer Misuse and Cybercrimes Act 19 of 2020, s 17.

[92] Electronic Communications and Transactions Act 25 of 2002.

(ECTA), 2002[93], provides a foundational legal framework for digital transactions, ensuring consumer protection in online spaces and establishing provisions related to data security, encryption, and cybercrime offenses. Collectively, these institutions and legislative measures strengthen South Africa's approach to promoting and protecting personal user data within the cybersecurity landscape**.**

With regard to its judicial approaches, in *Black Sash Trust v Minister of Social Development & Others [2017]*, the South African Social Security Agency (SASSA) and its outsourced service providers were required by the Constitutional Court to safeguard beneficiaries' personal information against unauthorised use by third parties[94]. The court reinforced the principle that state entities handling personal data must ensure compliance with data protection regulations and safeguard citizens' rights.

Another significant case is *Amabhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others [2021]*, where the Constitutional Court ruled that aspects of South Africa's surveillance laws were unconstitutional as they failed to provide adequate safeguards against arbitrary interception of personal communications[95]. The ruling emphasized that data surveillance measures must adhere to constitutional protections and international best practices.

4.4 Lessons Kenya Can Learn from South Africa

i. Strengthening informed consent:

By demanding explicit and informed consent before processing personal data, POPIA ensures that users have total control over their data[96]. People's control over their personal data is strengthened by the opportunity to withdraw consent at any time[97].

[93] Electronic Communications and Transactions Act, No. 25 of 2002 (South Africa).

[94] *Black Sash Trust v Minister of Social Development & Others* [2017] ZACC 8.

[95] *Amabhungane Centre for Investigative Journalism NPC v Minister of Justice* [2021] ZACC 3.

[96] Protection of Personal Information Act 4 of 2013 (South Africa) s 11.

[97] Protection of Personal Information Act 4 of 2013 (South Africa) s 5.

Consent clauses are included in Kenya's DPA 2019, although enforcement must be improved to ensure that companies have clear, unambiguous consent rather than relying on vague or generic language in privacy policies[98].

ii. *Comprehensive Categorization of Privacy Violations*

POPIA explicitly states that inappropriate use, excessive processing, and unlawful data collection are examples of privacy issues[99].

It provides clear legal consequences for excessive surveillance and improper data handling[100].

Kenya should expand its enforcement capabilities to tackle subtle privacy violations, such as the use of secondary data (profiling and behavioural surveillance) and the data minimisation principles mentioned by Solove[101].

iii. *Enhancing Data Subject Rights and Remedies*

Under POPIA, people have a number of rights, such as the opportunity to see data, request that it be updated or removed, and challenge automated decision-making[102]. It is required of organisations to notify users about the processing of personal data[103]. Although nothing is known about it, Kenya's DPA offers comparable rights. The government must do more to encourage digital literacy and ensure that companies are providing clear, intelligible privacy declarations[104].

iv. *Establishing a Stronger Enforcement Authority*

[98] Data Protection Act No. 24 of 2019 (Kenya) s 32.

[99] J. Smith, *Data Protection Law in South Africa* (Oxford University Press 2021) 45.

[100] L. Mathews, 'Surveillance and Privacy: The Role of POPIA' (2020) 34 *South African Journal of Law* 198.

[101] Daniel Solove, *Understanding Privacy* (Harvard University Press 2008), 74.

[102] M. Van der Merwe, 'POPIA and Data Subject Rights' (2021) 56 *Journal of African Data Protection* 67.

[103] B. Kitur, *Digital Privacy in Africa* (Strathmore University Press 2022) 89.

[104] A. Wanjiru, 'Kenya's Data Protection Act and its Implementation Challenges' (2021) 10 *East African Law Review* 45.

The Information Regulator (IR) in South Africa has broad enforcement powers, including the capacity to conduct audits, issue penalties, and require corrective measures[105]. For disobedience, POPIA enforces harsh penalties, including criminal liability[106].

To guarantee stricter compliance monitoring and faster reaction to data breaches, Kenya's Office of the Data Protection Commissioner (ODPC) should be granted greater autonomy and enforcement power[107].

v. *Strengthening Cross-Border Data Transfer Regulations*

POPIA restricts cross-border data transfers unless the target country has similar legal protections or the data subject consents[108].

Kenya's DPA has protections for cross-border data transfers, but enforcement is currently deficient. Kenya can take a cue from South Africa, which demands stricter laws governing data localisation or adequate security measures when transmitting data overseas[109].

vi. *Addressing Surveillance and Government Overreach*

POPIA's oversight of state surveillance ensures that government agencies do not abuse their power to collect personal data[110].

The use of personal information by law enforcement for monitoring has sparked concerns about surveillance in Kenya. The government should impose stricter legal frameworks to ensure judicial scrutiny before collecting personal data and to stop widespread monitoring[111].

[105] T. Naidoo, *Regulating Data Protection: The Role of Information Regulators* (Juta 2020) 78.

[106] C. Moyo, 'Enforcement Mechanisms under POPIA' (2021) 40 *South African Law Journal* 301.

[107] P. Omondi, *Data Governance in Kenya* (Nairobi University Press 2022) 155.

[108] R. Dlamini, 'Cross-Border Data Transfers under POPIA' (2020) 33 *African Journal of ICT Law* 211..

[109] J. Ouma, 'Data Localisation in Kenya: Lessons from South Africa' (2023) 8 *Journal of Digital Policy* 99.

[110]S. Khumalo, *State Surveillance and Privacy Rights in South Africa* (Cape Town University Press 2021) 143..

[111] L. Muthoni, 'Legal Safeguards Against Government Overreach in Kenya's Data Protection Framework' (2022) 12 *East African Law Journal* 77.

4.5 Conclusion

With the passing of the Data Protection Act, 2019, Kenya has made tremendous progress; nonetheless, the more progressive legislative environment of South Africa is quite revealing. Kenya may develop its legal system to strengthen protection of personal data and uphold constitutional privacy rights in the information age by instituting tighter institutional control, promoting strategic litigation, and implementing best practices from South African law.

CHAPTER 5: CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

The chapter concludes this research by expounding on the conclusions derived from the study and offering recommendations that may help strengthen the legislative framework and its enforcement to better protect personal user data and the right to privacy in Kenya.

The first chapter set to introduce the research problem , presented the research questions that would be answered and the hypothesis upon which the research would be based on. The second chapter delved into discussing the legal framework personal user data. Chapter three discussed what constitutes challenges and gaps that undermine the effectiveness of Kenya's legal framework. Chapter four constituted an analysis of laws governing personal user data protection in South Africa and lessons which Kenya can learn from the South Africa.

The chapter concludes this research by expounding on the conclusions arrived at during the study and offering recommendations that may help remedy the problem.

5.2 Conclusion

This right is recognised as a fundamental human right by Article 31 of the Kenyan Constitution, which is backed internationally by documents like the Universal Declaration of Human Rights of 1948. However, due to the fast growing use of technical breakthroughs and the inadequate implementation of cybersecurity measures, the same is made vulnerable with rising dangers in this digital era.

Thus, this study found that although Kenya has worked to achieve data protection through laws such as the Data Protection Act, 2019, there are still implementation and public awareness gaps. The full realisation of privacy rights has been impeded by institutional capacity limitations, ambiguous jurisdictional boundaries, and inadequate penalties for violations. Additionally, it demonstrated that the harmonisation of international standards similar to the GDPR is not complete, allowing for improvement in a number of areas, including user consent, data breach reporting, and cross-border data transfers.

The study also pointed out that several public and private organizations are failing to implement effective mechanisms of cybersecurity, thus putting the users' data in grave jeopardy. Poor funding

and absence of comprehensive implementation plans are additional factors that heighten these risks. In addition, the sensitive data of security is also compromised due to a lack of industry-specific regulations corresponding to high-risk industries such as financial services and healthcare.

The government of Kenya should adopt a multi-faceted approach: from strengthening its laws to enhancing the mechanism of enforcement, creating public awareness to integrating technology-driven solutions for ensuring that the legislative framework correctly protects the right to privacy.

5.3 Recommendations

i) Strengthen the Enforcement of the Data Protection Act 2019

Although the Data Protection Act of 2019 provides a solid basis for safeguarding user data, its application requires reinforcement through:

- Increased resources and financial support for the Data Protection Commissioner's office.
- Enhanced instruction for judges and law enforcement personnel on cybersecurity and data protection topics.
- The creation of precise rules for carrying out the Act's provisions, particularly those pertaining to data breach management and fines for noncompliance.
- To respond to data breaches, a distinct team should be set up to look into and address privacy concerns right away.

ii) Align Legislation with International Standards

To guarantee strong user data privacy, Kenya should bring its cybersecurity and data protection legislation closer to international norms like the GDPR. This comprises:

- Requiring transparent opt-in procedures and explicit user consent for data processing.
- Establishing strict deadlines for informing impacted users and the appropriate authorities about data breaches.

- Putting in place protections for cross-border data transfers to guarantee that user information is safe even when exchanged across borders.
- Requiring businesses that handle significant amounts of sensitive data to conduct frequent privacy impact assessments (PIAs).

iii) Foster Public Awareness and Stakeholder Collaboration

To inform the public about their rights to privacy and how to protect their personal information, awareness campaigns are crucial. This can be accomplished by:

- Efforts for public education that the ODPC has undertaken in partnership with civil society organisations.
- Curriculums that incorporate cybersecurity awareness and data protection.
- Cooperation with the private sector to advance cybersecurity and data handling best practices.
- Creating a nationwide "Data Privacy Day" to raise awareness and stimulate discussion about privacy-related topics.

iv) Build Institutional Capacity

Institutional capacity is critical for effective implementation and enforcement of privacy laws. The government should:

- Invest in IT infrastructure so as to learn about, and reduce, cybersecurity threats.
- The personnel in the ODPC and other relevant bodies should be regularly trained.
- Establish specialized law enforcement units dedicated to dealing with cybersecurity offences.
- Create a centralized database that will account for reported data breaches in order to enhance accountability and transparency.

v) Promote Regional and International Collaboration

Kenya should actively engage in regional and international partnerships to fortify its legal and enforcement frameworks, considering the worldwide scope of cybersecurity threats. This includes:

- Collaborating in the creation of uniform cybersecurity regulations with other EAC nations.
- Interacting with international organizations in pursuit of technical support and best practice sharing.
- Signing agreements on mutual legal assistance in combating international cybercrime.
- Enhancing Kenya's ability to counteract transnational cyberthreats by joining international frameworks like the Budapest Convention on Cybercrime.

vi) Encourage Research and Innovation

Research and development should be funded by the public and private sectors to provide innovative cybersecurity technology and solutions. This can be achieved through:

- Encouraging academic research on data security and cybersecurity.
- Providing incentives for tech companies to develop innovative privacy-enhancing solutions.
- Establishing partnerships between the public and private sectors to address emerging cybersecurity challenges.
- Establishing innovation hubs dedicated to developing AI-driven instruments for detecting and preventing data breaches.

- Introduce Sector-Specific Regulations

To address the unique privacy challenges faced by different industries, Kenya should introduce sector-specific regulations. These could include:

- Stricter data protection standards for financial institutions to safeguard sensitive customer information.
- Enhanced cybersecurity protocols for healthcare providers to protect patient records.

- Tailored guidelines for educational institutions to ensure the safety of student data in digital learning environments.

These recommendations, when effected, will go a long way in assisting Kenya in advancing and defending the right to privacy in the digital era, with its legal and enforcement frameworks robust, all-inclusive, and in line with the best practices globally. Further, Kenya will be set to position itself as a leader in the area on digital governance if it takes a proactive approach to implementing technology advancements and cultivating a culture of privacy.

BIBLIOGRAPHY

Legal Instruments

Kenyan Laws

- Constitution of Kenya, 2010.
- Data Protection Act, No. 24 of 2019.
- Data Protection (General) Regulations, 2021.
- Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021.
- Data Protection (Complaints Handling and Enforcement Procedures) Regulations, 2021.
- Computer Misuse and Cybercrimes Act, No. 5 of 2018.

South African Laws

- Constitution of the Republic of South Africa, 1996.
- Protection of Personal Information Act, No. 4 of 2013.
- Cybercrimes Act, No. 19 of 2020.
- Electronic Communications and Transactions Act No. 25 of 2002.

International and Regional Instruments

- General Data Protection Regulation (EU) 2016/679.
- Universal Declaration of Human Rights, 1948.

Case Law

- *Okoiti v. Communications Authority of Kenya*
- *Bloggers Association of Kenya (BAKE) v. Attorney General & Others* (2020) eKLR.
- *Okoiti v. Communications Authority of Kenya*
- *Nubian Rights Forum & Others v. Attorney General & Others* (2020) eKLR.
- *Kenya Human Rights Commission v. Communications Authority of Kenya & Others* (2018) eKLR.
- *Okiya Omtatah Okoiti v Communications Authority of Kenya & Others* [2018] eKLR.
- *Bharat Thakrar v WPP Scangroup PLC* [2021] ODPC.

- *Black Sash Trust v Minister of Social Development & Others* [2017] ZACC 8.
- *Amabhungane Centre for Investigative Journalism NPC & Another v Minister of Justice & Others* [2021] ZACC 3.
- *Hájovský v. Slovakia* [2021] ECHR.
- *Warren v DSG Limited* [2021] EWHC 2168 (QB).

Books

- Calo, R., *The Law of Robots: Technology, Automation, and the Regulation of Future Societies* (Harvard University Press, 2021).
- Crawford, K., *The Hidden Biases in Big Data* (Yale University Press, 2021).
- Kaspersen, A. P., & Russell, S., *The Human Imperative: Power, Freedom, and AI in a Digital Age* (Oxford University Press, 2023).
- Kuner, C., *Transborder Data Flows and Data Privacy Law* (Oxford University Press, 2013).
- Nissenbaum, H., *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford University Press, 2010).
- Solove, D. J., *A Taxonomy of Privacy* (Harvard Law Review, 2006).
- Solove, D. J., *Understanding Privacy* (Harvard University Press, 2008).
- Westin, A. F., *Privacy and Freedom* (Atheneum, 1967).

Journal Articles

- Cate, F. H., 'The Challenge of Information Privacy' (2006) 44(4) *International Journal of Law and Information Technology* 231.
- Koops, B. J., 'The Trouble with European Data Protection Law' (2014) 4(2) *International Data Privacy Law* 250.
- Nissenbaum, H., "Contextual Integrity and the Protection of Personal Data" (2019) 32 *Ethics and Information Technology* 1.
- Solove, D. J., "A Taxonomy of Privacy" (2006) 154 *University of Pennsylvania Law Review* 477.
- Westin, A. F., "Social and Political Dimensions of Privacy" (1970) 59 *Journal of Social Issues* 431.

Reports and Official Documents

- Communications Authority of Kenya, *Annual Report on Cybersecurity and Data Protection in Kenya* (2022).
- European Commission, *Evaluation of GDPR Implementation Across Member States* (2021).
- Information Regulator (South Africa), *Annual Report 2022*.
- Kenya Human Rights Commission, *Data Protection in Kenya: Gaps and Challenges* (2020).
- Kenya ICT Authority, *National Cybersecurity Strategy 2022*.
- Kenya Law Reform Commission, *A Review of the Data Protection Legal Framework in Kenya* (2021).
- Office of the Data Protection Commissioner, *Annual Report on Data Protection Compliance in Kenya* (2022).

Theses and Dissertations

- Muriuki, J., 'The Effectiveness of Kenya's Data Protection Act in Safeguarding Digital Privacy' (LLM Thesis, University of Nairobi, 2021).
- Mutua, B. K., "Legal Gaps in Kenya's Cybersecurity Framework: A Comparative Study with the GDPR." (Master's Thesis, University of Nairobi, 2022).

Policy Papers and Other Documents

- East African Community, 'Regional Framework on Cybersecurity and Data Protection' (Policy Report, 2023).
- Kenya Bankers Association, 'Data Security in Kenya's Financial Sector' (Policy Paper, 2022).

Online Sources

- Communications Authority of Kenya, "Cybersecurity Threat Landscape in Kenya" (2023) https://www.ca.go.ke accessed [2023].
- European Data Protection Board, "Guidelines on Data Protection Impact Assessment" (2021) https://edpb.europa.eu accessed [2021].

- International Association of Privacy Professionals, "Cybersecurity Trends and Legal Developments in Africa" https://iapp.org accessed [date].
- Kenya Law Reports, 'Data Protection Act 2019' (Kenya Law, 2019) <www.kenyalaw.org> accessed [2019].
- Office of the Data Protection Commissioner, Kenya, "Data Protection Compliance Guidelines" https://www.odpc.go.ke accessed [2024].