UNIVERSITY OF NAIROBI

SCHOOL OF LAW

BY:

REG NO: G62/6991/2017

SUPERVISOR: DR. PETER GITAHI MUNYI

DATA PROTECTION AS A HUMAN RIGHT: BALANCING THE RIGHT TO PRIVACY AND NATIONAL SECURITY IN KENYA

DECLARATION

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

Signed: ……..

Date: ……..

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

Signed: ……..

DR. PETER GITAHI MUNYI

THE UNIVERSITY OF NAIROBI.

Date: ……

DEDICATION

This project is dedicated to my beloved wife, my daughter and my parents for their positive emotional and financial support while conducting this entire research project.

ACKNOWLEDGEMENT

God Almighty, the creator, you are acknowledged.

It is with sincere gratitude that I thank my immediate family for their emotional backing and financial contribution towards the completion of this research.

I am also grateful to my class mates for their positive attitude and constructive criticism in conducting this entire project.

My heart full thanks to my supervisor Dr. Munyi for his valuable guidance during the tenure of my research.

I would also want to acknowledge the support I got from the entire staff of Kenya National Library Services and The University of Nairobi, parklands campus library, who provided me with relevant texts and allowed me to conduct my research within their precincts. The staff of K & K Advocates LLP are acknowledged for their material support in the course of the research.

Above all I conclude my acknowledgement with express gratitude to the entire law faculty for being so resourceful and enabling me complete my research project within the required time.

TABLE OF CONTENTS

INTRODUCTION 7
Background of Study 7
Statement of the Problem 12
Justification of the Research. 14
Statement of Objectives 15
Research Questions 15
Hypothesis 16
Theoretical Framework 16
Literature Review 18
Research Methodology 21
Chapter Breakdown 22
CHAPTER TWO 23
CONSTITUTIONAL AND STATUTORY FRAMEWORK ON THE RIGHT OF PRIVACY IN KENYA 23
Introduction 23
Constitution of Kenya, 2010 26
International Law 35
Statutory Laws 36
The Computer Misuse and Cybercrimes Act 36
Kenya Information and Communications Act 38
National Intelligence Service Act 40
Conclusion 42
CHAPTER THREE 43
NECCESSITY OF GOVERNMENT SURVEILLANCE 43
Introduction 43
Reasonability, Proportionality and Necessity 44
Impact of Government Surveillance on Human Rights 47
Role of Non- State Actors in prevention of Interception and Data Protection 49
Conclusion 51
CHAPTER FOUR 52
COMPARATIVE ANALYSIS 52
Introduction 52
USA 53

European Union 55
South Africa 59
Conclusion 59
CONCLUSION AND RECCOMENDATIONS 60
Introduction 60
Conclusion 60
Recommendations 62
BIBLIOGRAPHY 66

CHAPTER ONE

INTRODUCTION

Background of Study

Privacy is an important component in life as it affects how individuals behave, act and make choices.[1] It acknowledges the respect and autonomy of human beings.[2] The right to privacy has been highly upheld by diverse societies and developed from a common law right to a universally accepted human right.[3] Intrusion of the right is considered as a spiritual harm that must be addressed by law.[4] This has necessitated the need to put more strict measures to protect the right to privacy.[5] However, these measures have always considered the need to protect other rights. This has therefore required the need to understand the value of privacy in order balance competing interest.[6]

The right to privacy is explicitly provided under the Constitution of Kenya, 2010. The Constitution highly safeguards the right to privacy among the numerous fundamental freedoms and rights that are guaranteed under the Bill of Rights. Under Article 31(a), one cannot be arbitrarily searched including his home and property. Under sub-article (b) and (c), one's information relating to family and private affairs cannot be unnecessarily revealed or the privacy of one's communication infringed. There are six core items in the protection of the right to privacy. These are one's right to be left alone, limitation of access to one's private life, secrecy,

[1] Andrew Serwin,' Privacy 3.0-The Principle of Proportionality,'(2009) 42 University of Michigan Law Journal , page 872
[2] Ibid
[3] Lyn Entrikin, 'The Right to Be Let Alone :The Kansas Right of Privacy,' (2014) 53 Washburn Law Journal, page 208
[4] Richard Bruyer,' Privacy : a Review and Critique of the Literature,'(2006) 43 Alberta Law Review , page 556
[5] Ibid
[6] Ibid

control of collection, use and dissemination of personal information and protection of one's integrity and dignity.[7]

The right to privacy is best presented in the negative. It involves the right not to be unnecessarily invaded. Thomas Cooley described the right to privacy as the right to be left alone.[8] The necessity of protecting the information of one's private life is due to the fact that the information can be used to injure one's personality.[9] This therefore requires that information of one's private life be highly protected.[10] To protect one's privacy in the modern age, one has to be able to control the accessibility of information on one's private life.[11]

The growth of internet and technological developments through innovations and inventions have widely increased platforms for communications and database for personal information. [12] There has been a constant growth in collection of data from individuals due to the rapid and endless advancement of technology.[13] This growth has also increased intrusion to the sacred precincts of the right to privacy.[14] Surveillance technology systems also pose a major threat to the right to privacy.[15]Technological growth has brought in an era of big data which comprises of collection and analysis of large pieces of personal data and created the urgency in law to provide remedy

[7] Daniel Solove, 'Conceptualizing Privacy,'(2002) 90 California Law Review , page 1094
[8] Major Harding, Mark Criser & Michael Ufferman,' Right to be let Alone? Has Adoption of Article 1 , Section 23 in the Florida Constitution , which Explicitly Provides For a State Right to Privacy, Resulted in Greater Privacy Protection for Florida Citizens?,'(2014) Notre Dame Journal of Law, Ethics & Public Policy, , page 945
[9] Dorothy Glancy, 'The Invention of the Right to Privacy,'(1979) 21 Arizona Law Review , page 4
[10] Ibid
[11] Hannah Yee Fen, 'The Data Protection Paradigm for the Tort of Privacy in the Age of Big Data,'(2015) 27 Singapore Academy of Law Journal, page 790
[12] Samuel Warren & Louis Brandies,' The Right to Privacy ,'(1890) 4 Harvard Law Review , , page 194
[13] Jody Ferris,' Data Privacy and Protection in the Agriculture Industry :Is Federal Regulation Necessary?,'(2017) 18 Minnesota Journal of Law, Science & Technology, page 309
[14] Ibid
[15] Ashok Kumar, 'Surveillance and Right to Privacy :Issues and Challenges,' (2017) 3 International Journal of Law , page 74

from unauthorized access, use and dissemination of data that can be considered private and control how personal information is collected, used and disseminated.[16]

The rise in technological development and surveillance requires the Constitution and applicable laws to adopt an interpretation that responds to the emerging issues. Both public and private bodies collect personal information. Even though the information might be given with one's consent, the intention is that the information is used solely for the purpose it was given and not disseminated without the consent of the giver. The collectors of the information have a duty to secure and protect the information and not give it to any other person without consent. Article 31 of the Constitution points out clearly one has the right to give or not to give personal information unless it is necessary. To ensure protection of privacy, it requires legal measures on data protection measures to enable sufficient control of collection, use and dissemination of information that can be considered private.

Data protection enables one to among others, choose freely how their personal information can be exposed.[17] Data protection laws need to address the threats posed by technology that has widened access to personal data. This requires that data protection has to be beyond just collection, use and dissemination but also capture surveillance especially by the government.[18] In recent times there has been increase in government surveillance.[19] This has severely exposed the privacy of personal information.[20]

[16] Fred Cate, Christopher Kunner, Christopher Millard & Dan Jerker ,'The (Data Privacy) Law Hasn't Even Checked in When Technology Takes Off,'(2014) Articles by Maurier Faculty, page 180
[17] Jed Rubenfeld, 'The Right to Privacy,'(19890 102 Harvard Law Review , page 741
[18] David Flaherty,' On the Utility of Constitutional Rights to Privacy and Data Protection,'(1991) 41 Case Western Law Review, page 849
[19] Eliza Watt, 'The Right to Privacy and the Future of Mass Surveillance,'(2016) 21 International Journal of Human Rights, page 776
[20] Ibid

Both public and private bodies, who are in a position to collect, store and disseminate data are custodians of personal information they have received and they have a duty to protect the information.[21] The government is the biggest custodian of personal information since it handles more personal information than any other institution.[22] Other than the usual collection of personal information in the course of delivering services, governments have been involved in surveillance and interception of private conversations of its citizens.[23] Even though the government has justified the interception and surveillance on grounds of national security, in most occasions, it has been indiscriminate and gone even beyond territorial borders.[24] The government interception of private conversations and invasion of private information is an infringement of the right to privacy where it is unnecessary and unreasonable.[25]

The state acts the duty bearer in the protection of human rights[26]. The Constitution provides that the state is mandated to ensure that all persons enjoy their rights and that one person's right does not affect the enjoyment of the rights of others. As a duty bearer, the state has to put in place strict measures to protect the right to privacy through data protection. Article 21 requires the State to protect, observe, respect and fulfill the fundamental rights and freedoms. The obligation to respect requires the state not to interfere with ones right. To protect, it requires the State to prevent non state actors from infringing on the rights and to fulfill requires the state to take positive measures to facilitate their realization.

---

[21] Stefan Schuster, Melle Berg, Tom Slewe & Peter Kostic,' Mass Surveillance and Technological Policy Options : Improving Security of Private Communications,' (2017) Computer Standards & Interfaces, page 77

[22] Ibid

[23] Rachel Waldman ,'Government Access to and Manipulation of Social Media :Legal and Policy Challenges,'(2018) 61 Harvard Law Journal , page 525

[24] Asaf Lubin, 'We Only Spy of Foreigners : The Myth of a Universal Right to Privacy and the Practise of Foreign Mass Surveillance,'(2018) 18 Chicago Journal of International Law, page 507

[25] Will Thomas, 'Protecting Privacy in Digital Age,' (2003) 18 Berkeley Technology Law Journal, page 284

[26] Johaness Morsink,' Inherent Rights : Philosophical Roots of Universal Declaration,' (2012) University of Pennsylvania Press page 128

There are three areas when it comes to privacy and data protection in government surveillance.[27] These are the interception of information, the limitation on the right to privacy from government intrusion and the provision of remedies from intrusion. The general rule is that the government should not intercept private communication and information as it is an intrusion of the right to privacy. It also means that corporates such as the telecommunications industry have a duty to protect the private data and private communications and should not surrender it to government unless it is highly necessary. Telecommunications companies have been undertaking more encryption to secure private information but have also been pressured to release private information or allow government intrusion in private communications.[28]

Article 19(1) clearly states that human rights are integral to Kenya as a democratic state. Right to privacy protects the sanctity, dignity and integrity of an individual.[29] It is a core right in any democratic state. The Constitution guarantees the right on each individual and subject to limitations based on the principles provided under Article 24. Article 20 requires that a right should be enjoyed to its greatest extent and hence the extent of limitation has to be reasonable and justifiable.

National security has operated as a ground to limit the right of privacy.[30] It is usually based on collection of intelligence. In the recent past there have been reports of extrajudicial surveillance by the government. The Kenya Information and Communications Act outlaws surveillance under Sections 31, 83 and 93. These sections majorly apply to private organizations and persons and not the government such as intelligence bodies as it applies to the telecommunications industry

[27] Gerald Cope ,'Toward a Right of Privacy as a Matter of State Constitutional Law,'(2014) 5 Florida State University Law Review, page 634
[28] Ibid No 22, page 81
[29] Jonathan Manes, 'Online Service Providers and Surveillance Law,'(2016) 125 Yale Law Journal , page 344
[30] Ibid

.The National Intelligence Service Act, The Prevention of Terrorism and Security Laws (Amendment) Act allow government surveillance. Even though there can be legitimacy in intruding on privacy for national security, it should be proper and necessary. There is no proper legal framework of oversight to ensure that the intelligence organs or any government institutions intrusion is necessary. Inadequate legal framework has led to unregulated surveillance. In USA, the judiciary plays a huge role in controlling government intrusion.[31]Indiscriminate mass surveillance is an infringement on the right to privacy in the USA jurisdiction. There have been reports especially by the civil society in Kenya of mass government surveillance. [32] This is especially with regards to infiltration of telecommunications network, sharing of information and surveillance for kill and capture.[33] Mass surveillance goes beyond the limits allowed in law. The Constitution has allowed intrusion only when it is necessary. It is important to clearly analyze the constitutional threshold of the term necessary.

Statement of the Problem

Kenya does not currently have specific data protection legislation. However, a Data Protection Bill was tabled in Parliament in 2015 and to date, the Bill has not yet passed. It has been said that a technicality led to its withdrawal from Parliament hence the delay. Once law, the Bill is meant to breathe life to Article 31(c) of the Constitution, which outlines the right of every person not to have "information relating to their family or private affairs unnecessarily required or revealed" and Article 31(d), the right not to have "the privacy of their communications infringed"[34]. It would also regulate the collection, retrieval, processing, storing, use and disclosure of personal

[31] Ibid No 27
[32] Privacy International,' Track , Capture , Kill : Inside Communication Surveillance and Counterterrorism in Kenya,' < https://privacyinternational.org/sites/default/files/2017-10/track_capture_final.pdf>
[33] Ibid
[34] https://privacyinternational.org/state-privacy/1005/state-privacy-kenya as accessed on 5th November, 2019

data. It is rather appaling that despite the public uproar, the proposed legislation does not explicitly address the protection of data stored in the "cloud" (synchronised storage centres for digital data). Many cloud repository servers are based outside Kenya, which further troubles the proposed legislation.

The major issue is that while progress has been made to protect personal information and interception of private communications from non-state actors, little progress has been made to protect Kenyan citizens from government surveillance. While intrusion of privacy can be limited for national security reasons, it should be done only when it is necessary. There have been reports of large scale surveillance in Kenya.[35] The existing laws do not provide judicial oversight in access to private information thus leading to the immense abuse by Government agencies that has been witnessed in the past.

A March 2017 investigation by Privacy International revealed that the NIS has direct access to Kenya's telecommunications networks, which allows for the interception of both communications data and content[36]. Direct access describes situations where state agencies have a direct connection to telecommunications networks which allows them to obtain digital communications content and data (mobile and/or internet) without prior notice or judicial authorisation and without the involvement of the telecommunications provider or internet service provider that owns or runs the network[37].

[35] Privacy International,' Track , Capture , Kill : Inside Communication Surveillance and Counterterrorism in Kenya,' < https://privacyinternational.org/sites/default/files/2017-10/track_capture_final.pdf>
[36] https://privacyinternational.org/state-privacy/1005/state-privacy-kenya as accessed on 5th November, 2019
[37] Ibid

In March 2012, the telecommunications industry regulator, the then-Communications Commission of Kenya (CCK, the precursor to the Communications Authority), announced that it was setting up a system to allow the authorities to monitor incoming and outgoing digital communications[38]. The CCK requested that all telecommunication service providers cooperate in the installation of internet traffic monitoring equipment; known as the Network Early Warning System (NEWS). The CCK cited a rise in cyber security threats as a justification for this move. NEWS is an initiative of the UN's International Telecommunication Union (ITU) to aggregate data on cybersecurity threats and disseminate it worldwide.

In January 2017, the Communications Authority (CA) announced a further three measures costing an estimated 2 billion KSh (15.2 million GBP) to monitor Kenyans' communications and communications devices. Among these was a "device management system" to detect fraudulent devices and a social media monitoring project. According to an investigation published in March 2017 by Privacy International, in late 2016, the CA finalized a contract with Israeli 'web intelligence' firm webintPro, according to CA sources[39]. It is legitimate to limit the right to privacy due to the growth of national security threats such as terrorism. However, the right to privacy should not be sacrificed. There is also the challenge of government institutions forcing private institutions such as telecommunications industries to provide backdoor access to private information. There is need for a constitutional basis that allows this collaboration where it is necessary. Reasonable access needs to be clearly defined.

Justification of the Research.

The growth of technology has increased platforms that have created channels for intrusion of privacy. However, this intrusion is legitimate if properly done for national security. It is

[38] Ibid
[39] Ibid

important to look at the boundaries to ensure that the right to privacy is not abused by intelligence services. Due to growth of terror threats in Kenya, there have been increase in reports of government surveillance. Government surveillance is legitimate if done under the correct legal and institutional framework that provides for judicial oversight. The government does not only conduct surveillance but can also collect information from the citizens. Measures to protect privacy through data protection are also important. This is because the government may seek to access personal data held by corporates or private organizations. The research seeks to look into these since it is an emerging area in modern era.

Statement of Objectives

The main objective of this research is to define the balance between the right to privacy and its limitations for the purpose of national security. In order to achieve this objective, a number of sub-objectives have been derived. These are presented herein below.

1. To the define constitutional and statutory basis for limitations of data protection and the right to privacy
2. To define which government intrusion of privacy is constitutionally necessary
3. To define the role of non-state data collectors in protecting private data
4. To establish how other jurisdictions have approached the right to privacy and national security

Research Questions

The questions this thesis seeks to look at are

1. What is the constitutional and statutory basis for limitations of data protection and the right to privacy?
2. Which government intrusion to privacy is constitutionally necessary?

3. What is the role of non-state data collectors in protecting private data?
4. How have other jurisdictions approached the right to privacy and national security?

Hypothesis

The research is based on the following hypothesis

1. That government has a mass surveillance system with no proper oversight
2. That modern technology has a lot of backdoors that allows infringement of the right to privacy
3. That non-state actors who hold private information have no mandate to allow government access to private information

Theoretical Framework

Expressive Theory

The Expressive theory posits that law enables reconstruction of norms.[40] This can express societal hopes, goals, fears and attitudes. The law on privacy sends a message that people are safe and their information cannot be misused. The laws that allow intrusion shows lack of respect for the dignity of citizens. It curtails liberty. The higher it allows intrusion, the more it becomes emphatic on government's respect for human rights. One of its proponents, Hellen Nissnbaum posits that privacy is violated when government goes beyond the limits. She states that in privacy there are four key items, the actors, the process of access to information and its control, the frequency of access and the purpose of access. The law must consider the four items when putting limitations. This requires that wrong actors should not be allowed, access and frequency should be controlled and purpose of access must be known.

[40] Craig Konnoth, 'The Expressive Theory of Privacy Intrusions,'(2017) 102 Iowa Law Review , page 1537

Intrusion can have harmful consequences hence the need for protection of privacy. Where there is no protection, it creates the fear in one expressing oneself and this can prevent a society from developing maturity. State action affects behavior. It shapes the relationship between the surveilled and the surveillors. Intrusions suggest that one lacks social standing. Even when victims are not conscious of the intrusion, it does affects the perceived status in the eyes of observers. This can also be linked with the equality theory as mass surveillance in jurisdictions such as USA has made women more susceptible to suffer intrusions.

However, based on the utilitarian theory, the research does not call for total abolishment of surveillance. There may be need for surveillance especially those involved in terrorism for the greater good of the society. Therefore, surveillance has to be carried out in an environment that only allows surveillance for legitimate reasons and must consider the harms it can bring tp an individual.

Tragedy of the Commons

The theory of tragedy of the commons with regards to privacy applies to modern technology and intrusion of privacy. The internet is accessible to a wide range of people with highly uncontrolled access to private information. This is especially with regards to the social media. The theory posits that common resource is usually depleted and uncared for due to the common access.[41] This allows easier intrusion of privacy. This therefore requires that a law defines roles to ensure collectors of information in the internet protect private information and prevent intrusion. This calls for encryption even in restricting government access. Fairfield and Engel posits that regulation is limited in protecting privacy as individual control of ones data is fundamentally

[41] Smith Grinell & Rabin Colette,' Modern Education : A Tragedy of Commons,' (2013) 45 Journal of Curriculum Studies, page 749

flawed.[42] They say privacy can be sufficiently protected by allowing groups of people to coordinate their actions in privacy protection.

Under tragedy of the commons, Fairfield and Engel argue that individual decision to disclose personal information affects the privacy of others.[43] The over use in disclosure of personal information leads to tragedy of the commons. However, Fairfield and Engel call for the tragedy of the trust resource.[44] In this tragedy, they speak of those who have been given personal data. They state that these institutions that have collected personal information, have a mandate to protect it. They state that the information economy relies on digital trust therefore any information shared ought to be protected from intrusion even by the government.

Literature Review

There are many writers who have canvased on the area of privacy and national security. *Stefan, Melle, Tom* and *Peter* make a deep analysis on mass surveillance by governments on private communications.[45] They focus on the USA jurisdictions after the Snowden revelations.[46] They argue that they USA conducted mass surveillance which was a direct infringement of the right to privacy. They state that the issue of government surveillance in the current technological era has been handled inadequately. They argue that instead of governments protecting the right to privacy, most governments have increased surveillance therefore infringing the right. They suggest that there is need for companies to enhance encryption to prevent surveillance and protect the right to privacy. They conclude that the protection of privacy requires collaboration

[42] Joshua Fairfield & Christoph Engel ,'Privacy as a Public Good,'(2015) 65 Duke Law Journal , page 385
[43] Ibid
[44] Dennis Hirsch, 'Privacy, Public Goods, and the Tragedy of the Trust Commons :A Response to Professors Fairfield and Engel,'(2016) 65 Duke Law Journal, page
[45] Stefan Schuster, Melle Berg, Tom Slewe & Peter Kostic,' Mass Surveillance and Technological Policy Options : Improving Security of Private Communications,' (2017) Computer Standards & Interfaces
[46] Edward Snowden was an employee of the Central Intelligence Agency who disclosed of mass surveillance programs run by the USA's government.

between government, companies and the public. The article however does not discuss the limitations of privacy for the purpose of national security.

Ashok Kumar[47] discusses widely on surveillance and the right to privacy. He says that the legislative framework that supports surveillance must be able to balance the right to privacy of an individual and the security and defense of a state. In his analysis, he shows how government surveillance in modern era has gone beyond border as far as Indians being monitored by intelligence bodies from as far as USA. Those that are not monitored are usually those who have not accessed the internet. The author widely discusses the legal approaches that states have taken in approaching the issue of surveillance. He states that restrictions have to be reasonable. The article gives a wide perspective on how the balance should be attained. It however does not cover the mandate of corporates in preventing access to personal information that this paper also addresses.

Richard Bruyer critiques various literatures on the right to privacy.[48] He discusses on a number of jurisdictions such as Canada on how he right out to be protected. Privacy is presented more of an equality issues rather than a liberty issue. The challenge is to take a change in the conceptual understanding of what is deemed as private. When presented as a liberty issue, liberty issues tend to conflict but equality issues do not. As an equality, it can easily accept limitation. As argued limitation strengthens realization of a right when done correctly. The article contributes to the discussion on the issue of privacy though it does not touch on the other issues of national security.

[47] Ashok Kumar, 'Surveillance and Right to Privacy :Issues and Challenges,' (2017) 3 International Journal of Law
[48]Richard Bruyer,' Privacy : a Review and Critique of the Literature,'(2006) 43 Alberta Law Review

Hannah Yee looks at the common law data protection regime.[49] The right to privacy has not been provided explicitly in the USA Constitution. However, the right to privacy has been protected through common law. This has been through common law torts. The common law torts has however been inadequate in ensuring proper protection of the la and most USA states and the European Union have adopted policies to protect the right to privacy. Common law torts is inadequate in the modern age of data collection.

Carol Nackenoff widely agrees that there is insufficient protection of the right to privacy in the modern era.[50] She discusses on the redefinition of the boundaries between public and private life. This calls for progressiveness in recognition of the private sphere of life away from government oversight and intrusion. Warren and Brandeis, who are recognized as great proponents and thinkers of the right to privacy foresaw the need to look at broader protection of the right to privacy with the development of technology. They called for progressive reforms.

Daniel Solove[51] discusses on conceptualizing the right to privacy. He proposes a new approach in concept. He argues that privacy ought not to be defined narrowly since it is built up of different characteristics. It is from these that legal solutions in protections of privacy can be formulated. The information age presents various challenges which require legal solutions that understand the concept of privacy.

Jonathan Manes looks at privacy specifically with regards to online service providers.[52] The article discusses on the role of tech companies where they have been required to provide access to government surveillance and in protection of privacy. The companies have a duty to inform

[49] Hannah Yee Fen, 'The Data Protection Paradigm for the Tort of Privacy in the Age of Big Data,'(2015) 27 Singapore Academy of Law Journal
[50] Carol Nackenoff,' Privacy, Police Power, and the Growth of Power in the Early Twentieth Century : A Not So Unlikely Coexistence,'(2015) 75 Maryland Law Review,
[51] Daniel Solove,' The Taxonomy of Privacy,'(2006) 154 University of Pennsylvania Law Review
[52] Jonathan Manes, 'Online Service Providers and Surveillance Law,'(2016) 125 Yale Law Journal

the public on government tools on surveillance. This aids in protection of the right to privacy. National security does not only affect the right to privacy it has also curtailed on the freedom of speech as tech-companies are prevented from informing their customers that the government has put the under surveillance.

The learned Justice John Mativo in deciding the case between Kenya Human Rights Commission and the Communication authority[53] is seen detailing the dangers of breach of privacy. He states "…'*The processing of information by the data user/responsible party threatens the personality in two ways: [22] a) First, the compilation and distribution of personal information creates a direct threat to the individual's privacy; and (b) second, the acquisition and disclosure of false or misleading information may lead to an infringement of his identity". This forms the basis of this paper in the Kenyan context.*

Research Methodology

This research is mainly theoretical in nature and hence it will use desk research methodology to gather data. It is based on research studies carried out previously and data from both public and private bodies. It will look into both primary and secondary sources of information through external desk based review. The primary sources of information mainly includes The Constitution of Kenya, 2010, The Computer Misuse and Cybercrimes Act , Kenya Information and Communications Act, International Covenant on Civil and Political Rights and National Intelligence Service Act. The secondary sources mainly includes books, journals and internet. The research will be qualitative in nature and will use grounded theory to analyse the research questions. It will also look into various case studies by analysing different jurisdictions and their approach to data protection.

[53] **Kenya Human Rights Commission v Communications Authority of Kenya & 4 others [2018] eKLR** at paragraph 54 of the judgment

Chapter Breakdown

Chapter One: This is the introductory chapter. It consist of the introduction, statement of the problem, justification and objective of the study, the research questions; the theories on which this paper is based on, the literature review of books and articles relied upon , the hypothesis research methodology and the chapter breakdown.

Chapter Two: The Second Chapter focuses on the constitutional and statutory basis for limitations on data protection and the right to privacy. This will delve into the legal framework and analyse its inadequacies. This will be focussed on answering the first research question.

Chapter Three: The third chapter will look into the necessity of government surveillance on the ground of national security. It will define the boundaries and also the role of non-state actor institutions such as telecommunications industry in protecting private data. This will be focussed on the second and third research questions.

Chapter Four: The fourth chapter will make a comparative analysis on the right to privacy and data protection with other jurisdictions mainly USA, European Union and South Africa. This will be focussed on the fourth research question.

Chapter Five: Recommendation and conclusion. This chapter shall make a conclusion of the study and outline the necessary recommendations.

CHAPTER TWO

CONSTITUTIONAL AND STATUTORY FRAMEWORK ON THE RIGHT OF PRIVACY IN KENYA

Introduction

The need for a legal framework on data protection emanates majorly from the right to privacy. It is also highly associated with national security, right to information and cyber security.[54] Data protection has become highly fundamental in the current era of big data as individuals seek to have better and enhanced control of their personal data.[55] It is widely seen to be synonymous and interchangeable with the right to privacy.[56] However, due to the growth of data and its importance, the right to data protection is being recognized as a separate right in many European jurisdictions.[57] This is however not the case in Kenya as there is no distinct provision for the recognition of the right to data protection independent from the right to privacy.

The school of thought of having the right to data protection as a distinct human right is to promote better enforcement, promote a proactive approach and make it more comprehensive.[58] It also elevates major principles of data protection putting obligations of data processors.[59] European jurisdiction has widely developed the right to data protection. Furthermore, its member states are making discussions on the right to be forgotten where one can require his or her personal information held by an organization to be wiped out.[60] This shows the different

---

[54] Orla Lynskey, *The Foundations of EU Data Protection Law*, (1st Edition, Oxford University Press, 2015), page 2
[55] Ibid
[56] Alex Makulilo,' Privacy and Data Protection in Africa: A State of the Art,' (2012) 2 International Data Privacy Law, page 177
[57] Ibid
[58] Ibid
[59] Yvonne McDermott,' Conceptualizing the Right to Data Protection in an Era of Big Data,' < https://journals. sagepub. com/doi/pdf/10.1177/2053951716686994 > accessed on 20th May 2017
[60] Napoleon Xantholis,' The Right to Oblivion in the Information Age: A Human-Rights Based Approach,' (2013) 10 US-China Law Review, page 85

dimensions through which the right to privacy and data protection is developing. Discourse on having data protection as a distinct right is highly likely to develop as Information, communication and technology industry advances.

As technology advances capturing, storing and using personal data, the need for data protection legal framework has become vital. The rise of information, communication and technology has catalyzed the concern for privacy.[61] ICT has caused massive collection of personal data that is under threat of breach where its misuse can result to harm . Data has become core across all industries from agriculture, retail, finance and healthcare. This has called for measures to create accountability on use of personal data.[62] The aim of having an elaborate and comprehensive data protection law is to ensure that the custodians of data take responsibility in managing people's personal data.

The government and corporates across all the economic sector are the major custodians of personal data.[63] Lack of care by government and corporate entities has exposed personal data to abuse and manipulation.[64]While the right of privacy has predominantly been used to protect undisturbed private life or information within one's private sphere, modern data protection is focused on the information that is not necessarily in private sphere.[65] It seeks to protect against unjustified use, collection, dissemination and storage of personal details.[66] The focus mostly on how private data is processed, stored and disseminated. This requires a legal framework that is enforceable and makes the custodians responsible.

---

[61] Ibid
[62] Ibid
[63] Menno Mostert, Annelin Bredenoord, Bart van der Sloot & Johannes van Delden,' From Privacy to Data Protection in the EU: Implications for Big Data Health Research,' (2017) 24 European Journal of Health Law, page 2
[64] Ibid
[65] Ibid
[66] Maria Tzanou, 'Data Protection as a Fundamental Right Next to Privacy? Reconstructing a Not So New Right,' (2013) 3 International Data Privacy Law, page 91

Cases of data breaches have immensely increased in the last five years.[67] This has exposed people to a myriad of risks including fraud, defamation, cyberbullying and cyber-attacks.[68] Cases of hacking have immensely increased.[69] Since the data breaches have increased , the safety of personal data is under great threat. Inadequate legal frameworks usually results in poor enforcement mechanisms against data breaches.[70] The Constitution of Kenya provides for the right of privacy and the parliament has a role to enact statutes to ensure full data protection.

Formulation of legal frameworks to ensure that organizations that collect information are accountable in storage and use of the information has become a necessity. However, the formulation of the law is affected by various interests. One is the balance between national security and the right to privacy. This has always been a contentious in many jurisdictions.[71] Government surveillance especially in heightened terrorist threats has resulted to deep limitations of the right to privacy. Two is the balance between the right to privacy and the right to information. This is with regards on which information the public can access and which can never be accessed on the basis that it is privileged or private.

The Constitution of Kenya and various statutes provides on matters of data protection. Kenya is in the process of enacting a statute to specifically address matters of data protection. Kenya is catching up with other jurisdictions as 107 states have already put a data protection legislation.[72]

---

[67] Consumers International, 'The State of Data Protection Rules Around the World: A Briefing for Consumer Organizations,' < https://www.consumersinternational.org/media/155133/gdpr-briefing.pdf > accessed on 17th May 2019

[68] Daniel Marcus,' The Data Breach Dilemma: Proactive Solutions for Protecting Consumers' Personal Information,' (2018) 68 Duke Law Journal, page 556

[69] Ibid

[70] Ibid

[71] Ioanna Tourkochoriti,' The Transatlantic Flow of Data and The National Security Exception in the European Data Privacy Regulation: In Search for Legal Protection Against Surveillance,' (2015) PAGE 460

[72] G.G Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (1ST Edition, Springer 2004) page 22

Most of these states are the developed states in North America, Europe and Asia.[73] Few states in Africa such as Niger, Burkina Faso, Mali, Chad, Angola, South Africa Zambia and South Africa have enacted statutes on data protection. The bill has borrowed a lot from the European Union's General Data Protection Regulation. This is also affected by recent measures by government to collect personal data for national security reasons. Below is an analysis of the current constitutional and statutory laws touching on privacy and data protection.

Constitution of Kenya, 2010

The Constitution of Kenya, 2010 is the supreme law of Kenya. Its validity is absolute and its provisions can never be challenged as provided under Article 2(3) of CoK, 2010. All sovereign power in Kenya is exercised through the Constitution as provided under Article 1. As the supreme law of the land, all written laws have to be consistent to the provisions of the Constitution. The data protection bill is required to be consistent with the provisions of the Constitution. CoK, 2010 also provides for national values and principles of governance under Article 10(2). The values under the provision that mostly relate to privacy and data protection are human dignity and human rights. Human dignity has been established as the foundation of the right to privacy.[74]

As a human right, the right to privacy is highly protected among other fundamental rights and freedoms. The Constitution of Kenya, 2010 provides for the bill of rights under chapter four. Under Article 21, every person and all the state organs.[75] Human rights are interventions of justice and reason to provide protection in an evil world.[76] The purpose behind protection of

[73] Ibid
[74] Luciano Florida,' On Human Dignity as a Foundation for the Right to Privacy,' (2016) Philosophy & Technology Journal, page 307
[75] Constitution of Kenya, 2010, Article 20
[76]Gunter Frankenberg,' Human Rights and the Belief in a Jus World,' (2014) 12 Oxford University Journal, page 37

human rights is in order to uphold human dignity, promote social justice and realize the human potential as provided under Article 19 (2). The Constitution provides that the bill of rights is an integral part of Kenya as a democratic state.[77]

Article 31 provides for the right to privacy. It provides four aspects with regard to the right to privacy. The person is not to be arbitrary searched. This is on the person, his or her home or property. This seeks to ensure that authorities and any other person does not interfere with one's private life including family.[78] This right has extended to not only individuals but also corporates. The second aspect is protection from seizure of possessions. This also affects the right to property and seeks to protect individuals from the state that can deprive the citizens off their property.[79]

The third aspect the right to privacy protects is information one's family being revealed or unnecessary required. It is under this limb of the right to privacy under the Constitution that data protection majorly applies. The right has been viewed as developing pursuant to the right to privacy.[80] The Constitution of Kenya , 2010 provides the right to data protection as a constitutive or a derivative right of the right to privacy. As discussed above, European Union has come to view the right to data protection and the right to privacy are rights that are closely linked

[77] Constitution of Kenya, Article 19
[78] Marius Emberland,' Protection Against Unwarranted Searches and Seizures of Corporate Premises Under Article 8 of the European Convention on Human Rights; The Colas Est SA vs. France Approach,' page 84
[79] Jose Alvarez,' The Human Right to Property, 'University of Miami Law Review, page 587
[80] LA Bygrave,' Data Protection Pursuant to the Right to Privacy in Human Rights Treaties, (1998) 6 International Journal of Law and Information Technology, page 254

but not identical rights.[81] International human treaties have also treated data protection as a subset of the right to privacy.[82]

The fourth aspect and final one is also related to data protection as it protects the privacy of one's communication. Communications, especially in this internet era covers, covers a wide aspect from telephone, mail and short message services. Interception of communication by the government , corporates and employees has been a serious infringement of privacy.[83] This has called for legal approaches to protect private communications especially by putting greater responsibility on telecommunications service providers.[84] This is especially by imposing liability.[85]

In ensuring that human rights are protected, the state acts the duty bearer in the protection of human rights[86]. Human rights are fulfilled when their correlative duties are performed and abused when those duties are not carried out.[87]CoK 2010 provides that the state is mandated to ensure that all person enjoy their rights. It is also required to ensure that one person's right do not affect the enjoyment of the rights of others. The state is required to protect, observe, promote, respect and fulfill the fundamental rights provided in the Constitution as provided by Article 21.it bears the greatest responsibility in human rights.[88]

---

[81] Juliane Kokott & Christophe Sobotta,' The Distinction Between Privacy and Data Protection in the Jurisprudence of the CJEU and the EctHR,' (2013) 3 International Data Privacy Law, page 228
[82] Orla Lynskey,' Deconstructing Data Protection: The Added Value of a Right to Data Protection in the EU Legal Order, page 570
[83] Sylvia Kierkegaard,' Privacy in Electronic Communication: Watch your Email, Your Boss is Snooping,' (2005) 21 Computer Law & Security Review, page 228
[84] James Griffin,' The Human Right to Privacy,' (2007) 44 San Diego Law Review, page 704
[85] Spiros Simitis, 'Privacy- An Endless Debate?' (2010) California Law Review, page 1992
[86] Johaness Morsink,' Inherent Rights: Philosophical Roots of Universal Declaration,' (University of Pennyslavania Press, 2012) page 128
[87] Natasa Mavriocola,' What is an Absolute Right? Deciphering Absoluteness in the Context of Article 3 of the European Convention on Human Rights,'(2012)12 Human Rights Law Review, page 729
[88] Naomi Arriaza,' State Responsibility to Investigate and Prosecute Grave Human Rights Violations in International Law,' (1990) 78 California Law Review, page 451

The Constitution also provides that the state shall enact and implement legislation to fulfill its international obligations in respect of human rights and fundamental freedom. If the state fails to uphold this obligations, Article 22 provides for enforcement of human rights through the court. Kenyans can also enforce their rights through court proceedings.[89] The Constitution grants the High Court the jurisdiction to hear and determine matters that involve human rights.[90]Courts across the globe especially in Europe and USA are having cases touching on data protection and the right to privacy.[91] This gives the courts great responsibility to safeguard privacy in the modern digital age.

Article 20 provides for application of human rights and provides that the court shall develop the law to the extent that it does not give effect to a fundamental freedom and also interpret the law in a manner that most favors its application. This is critical when the court needs to balance the right of privacy in circumstances where it is competing with other rights.

The Constitution has created a special body to aid in the promotion of human rights. This is the Kenya National Human Rights Commission. It is provided for under Article 59 with the mandate of promoting, protecting and monitor the status of human rights in Kenya. The Commission has been given wide tasks which includes to investigate and monitor the observance of human right, come up with reports on the observation of human rights by the state organs, receive and investigate complaints of human rights violations among other functions given through legislations.

[89] Constitution of Kenya, Article 22(1)
[90] Ibid Article 23
[91] Evangelia Psychogiopoulou & Maja Brkan,' Courts, Privacy and Data Protection in the Digital Environment,' in Evangelia Psychogiopoulou & Maja Brkan Courts, Privacy and Data Protection in The Digital Environment in the Digital Environment (1st Edition, Edward Elgar Publishing Limited, page 7

The right of privacy is regarded as a latecomer as it was recognized way later than other rights.[92] The right to privacy has clashed with other rights especially freedom of expression.[93] The Constitution provides for the freedom of expression under Article 33 where one can seek, receive or impart any information. Article 35 provides for the right to information. It gives every person the right to correct any untrue information about them. This is an aspect of data protection as it gives one the right to have any incorrect data corrected. The right to privacy is also among the rights that have been explicitly identified as rights that can be limited for persons serving in Kenya Defense Forces and National Police Service. This requires to undertake a strict balancing act in matters of rights to privacy and data protection.

The Constitution of Kenya, 2010 provides for limitation of human rights. Not all the rights provided in the Constitution of Kenya are absolute. The right to privacy is a derogable right as it is not among the rights in Article 25 of the Constitution. Article 25 provides for the non-derogable rights which are the right to a fair trial, freedom from slavery, freedom from torture and cruel, inhumane or degrading treatment or punishment and right to an order of habeas corpus. Having some rights as non derogable rights has always introduced the notion of hierarchy of human rights and made the principles of interdependence and indivisibility of human rights contentious.[94]

The state can derogate on the other rights as provided under Article 24 of the constitution. The Constitution provides that human right is guaranteed on each individual and subject only to the

[92] Thomas Emerson,' The Right of Privacy and Freedom of the Press,' (1979) 14 Harvard Civil Rights-Civil Liberties Review, page 329

[93] Dirk Voorhoof,' Freedom of Expression versus Privacy and the Right to Reputation,' in Stijn & Eva Brems, *When Human Rights Clash at the European Court of Human Rights: Conflict of Harmony?* (Oxford University Press, 2017)

[94] Teraya Koji,' Emerging Hierarchy in International Human Rights and Beyond: From the Perspective of Non Derogable Rights,' (2001) 12 European Journal of International Law, page 917

limitations provided in the constitution.[95]States can derogate in observing or respecting these rights majorly due to national security , proportionality or depending on exigencies of the circumstance.[96]

This means that the state has the obligation of limiting one's right in order to protect the right of others[97].Both the domestic and international legal framework provide for how the government is supposed to impose limitation on fundamental freedoms and rights.

The Constitution requires that the extent of limitation be reasonable and justifiable. The factors that have to be taken into consideration when considering limitation of rights include the nature of the right or fundamental freedom, importance of the purpose of the limitation, nature and extent of the limitation, the need to protect rights of others and relation between the limitation and its purpose and whether there are less restrictive means to achieve. It provides that the statute that seeks to limit freedom has to express the intention to limit the freedom the nature and the extent of limitation, the provision has to be clear and specific about the freedom that is being limited and that it should not limit the right or freedom so far as to derogate from its core or essential content.

The limitation clause provided in the Constitution is similar to the principles of limitations provided in the international instruments. The nature of a right validates its limitation.[98] It looks into both the subjective and the objective content of a right[99]. The objective content entails

[95] Ibid

[96] Kamal Hossain,' Methods of Dealing with Violations of Human Rights: What Needs to be Done and Why it is Not Done,' (1982) 9 Yale Journal of International Law, page 147

[97]Wouter Vandenhole,' Challenging Territoriality in Human Rights Law: Buildings Blocks for a Plural and Diverse Duty- Bearer Regime,' (2015) page 24

[98] Patrick Odhiambo,' Limitation of Rights under the Kenyan Constitution,' (LLM Thesis, University of Pretoria, 2015) page 26

[99] Gerhard Erasmus,' Limitation and Suspension of Human Rights,' (1994) Rights and Constitutionalism: The New South African Constitutional Legal Order page 629

looking at values and practices that are of essence in a democratic and constitutional society and the subjective are the values enjoyed either by an individual or a particular group of persons .[100]

The Final aspect of discussion on the Constitution is National Security. This is provided widely under Article 238 of the Constitution. The provision requires that national security respects human rights. One of the human rights that has been affected by national security principle is the right to privacy.[101] This is especially with regards to data privacy.[102] The imbalance the two is usually due to lack of checks and balances on the government especially the national security organs.[103]

In December 2016, the High Court in Nairobi declared unconstitutional a presidential directive seeking to collect names of people living with HIV, including names of school age children, among others[104]. Along with other organisations, the Kenya Legal & Ethical Issues Network (KELIN) had filed a case against a directive, arguing that the creation of this list was in violation with Article 31 and 53(2) of the Constitution, respectively, the right to privacy and the position that the "child's best interests are of paramount importance in every matter concerning the child[105]." There has been other instances of data breaches by the Kenyan government which have received massive airplay by the press. In December 2014, the Kenyan government arrested and expelled 77 Chinese citizens on suspicion of "preparing to raid the country's communication systems", according to the Police. Kenyan media reported that police raids had uncovered equipment

[100] Ibid
[101] Noorenanda Laidey,' Privacy vs National Security: Where Do We Draw the Line,'(2015) 9 International Journal od Social , Behavorial, Economic, Business and Industrial Engineering,' page 2235
[102] Ibid
[103] Ibid
[104] **Kenya Legal and Ethical Network on HIV & AIDS (KELIN) & 3 others v Cabinet Secretary Ministry of Health & 4 others [2016] eKLR**
[105] Ibid

capable of infiltrating bank accounts and government servers, as well as a popular banking system and ATM machines[106].

Reports from April 2016 indicate that hacker collective Anonymous breached the Kenyan Ministry of Foreign Affairs' servers and published 1 terabyte of files online. The Ministry later confirmed the hack as genuine and the result of junior staff members unknowingly giving access to the hackers by changing their passwords[107].According to the few civil society groups in Kenya who work on the issues, it is difficult to work on privacy and surveillance in the country as the issue is not widely deemed important. This is in part because an increased number of security threats has enabled a strong national security discourse to overshadow concerns about individuals' privacy. Privacy is often considered subsumed to other human rights issues[108].There are nevertheless serious concerns over disproportionate and unlawful surveillance in Kenya. In 2012, Peace Brigades International stated in relation to human rights defenders (HRDs) in Kenya that "incidences of surveillance by state and non-state actors have been reported. Offices have been raided or burgled and computers hacked, and several organisations suspected that their phones were being tapped." In October 2013, Human Rights Watch warned of the rising attacks on HRDs. Regular reports by the East and Horn of Africa Human Rights Defenders Project (EHAHRDP) and Front Line Defenders of HRDs and journalists being intimidated, attacked, arrested, tortured, killed, and kidnapped in Kenya demonstrate the significance of the issue.

[106] https://privacyinternational.org/state-privacy/1005/state-privacy-kenya as accessed on 5th November, 2019
[107] Ibid
[108] Ibid

During and in the aftermath of the March 2013 elections, the Kenyan government requested that mobile phone providers block text messages that were deemed to incite violence using a firewall that would detect messages containing key words, identified beforehand, to be further analysed. The National Steering Committee on Media Monitoring of the Ministry of ICT reportedly intercepted 300,000 texts messages daily during the 2013 elections[109].In July 2015, it was revealed that agents of the Kenyan intelligence services had contacted intrusion malware company Hacking Team to ask them to shut down a critical blog as a 'proof of concept' for their surveillance tools. The Kenyan government appeared to be attempting to procure the Remote Control System tool that allows for remote hacking and control of target devices.

The combination of these trends raises serious concerns about the government's potential use of surveillance tools to further repress civil society and human rights defenders, especially in the context of the 'war on terror,' which the government has used as a legitimizing narrative to justify serious human rights violations[110].

According to a March 2017 investigation by Privacy International, communications surveillance is being carried out by Kenyan state actors, essentially without oversight, outside of the procedures required by Kenyan law. Intelligence gained by intercepting phone communications, primarily by the NIS, is regularly shared with police units to carry out counter-terrorism operations, particularly the GSU-Recce company and Anti-Terrorism Police Unit (ATPU). These police units have well-documented records of abuses, including torture and extrajudicial killings. Information acquired from communications surveillance is central to the

[109] Ibid
[110] Ibid

counterterrorism cycle - from surveilling, profiling, locating, tracking and arresting targets to abuse, torture, abduction and extrajudicial killing.

International Law

The Constitution of Kenya under article 2(5) stipulates that the general rules of international law shall form part of the Kenyan law. It also provides in article 2(6) that the treaties and conventions that have been ratified by Kenya shall become part of the Kenyan law. Kenya has international obligations in fulfilling the provisions of the International treaties that it has ratified.

The EU General Data Protection Regulation is viewed as the most comprehensive international framework for data protection.[111]The UN adopted a resolution in 2013 that recognized the essence of the right of privacy in the digital age.[112] The right to privacy is well provided in United Declaration of Human Rights and the International Covenant on Civil and Political Rights. Article 8 of the United Declaration of Human Rights provides for the right to respect private and family life. Right to privacy is provided under Article 17. This touches the privacy of oneself, family and correspondence. There are also other instruments such as the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, UN Guidelines for the Regulation of Computerized Personal Data Files.

[111] Kathleen Paisley,' It Is All About Data: The Impact of the EU General Data Protection Regulation on International Arbitration,'(2018) 41 Fordham International Law Journal, page 841

[112] Kriangsak Kittichaisaree & Christopher Kuner,' The Growing Importance of Data Protection in Public International Law,' (2015) European Journal of International Law, page 2

Statutory Laws

The Computer Misuse and Cybercrimes Act

Kenya did not have a statute providing on the right to data protection before this Act was enacted. The Act was brought to address matters arising due to the technological development. The Act faced legal challenges in court when it was enacted. This was in the case of *The Bloggers Association of Kenya(Bake) vs. Attorney General and 5 Others.*[113]The court suspended 26 Sections pending full determination of the case. The Act has created offenses to prevent infringement of one's computer system. It provides for protection against unauthorized access under Section 14. Section 16 provides for unauthorized interference. Section 17 provides against unauthorized interception in transmission of data

The statute provides for offences related to computer systems. It provides for effective and timely detection, prohibition, prevention and response to the offences provided for. Where the detection and prevention cannot be avoided, it provides for investigation and prosecution of computer and cybercrimes. The Act also provides for international co-operation when dealing with cybercrime matters.

The Act's framework is similar to the Convention of Cybercrime, also known as the Budapest Convention on Cybercrime. This is a Treaty seeking to address internet and computer crime. It also serves as a guideline for any country developing legislation against cybercrime. The offences provided for are the same as the ones set out in the Convention, save for the provisions on intellectual offences through a computer system.

The Act establishes the National Computer and Cybercrimes co-ordination committee that will advise the government on security related matters touching on block chain, technology, critical

[113] [2018] eKLR

infrastructure, mobile money and trust accounts. The other function will be to advice the National Security Council on computer related and cybercrimes among other functions touching on reporting and developing a framework on matters cyber security.

The offences provided for in the Act are; unauthorized access, access with intent to commit further offence, unauthorized interference, illegal devices and access codes, unauthorized disclosure of password or access code, enhanced penalty for offences involving protected computer system, false publication, publication of false information, child pornography, computer forgery, computer fraud, cyber harassment, cybersquatting, identity theft and impersonation, willful misdirection of electronic messages, cyber terrorism, inducement to deliver electronic message, intentionally withholding message delivered erroneously, unlawful destruction of electronic messages, wrongful distribution of obscene or intimate images, fraudulent use of electronic data, issuance of false e-instructions, reporting of cyber threat, employee responsibility to relinquish access codes and aiding and abetting.

Cyber espionage is provided as an offence under the Act. This is the act of obtaining critical and sensitive information without the permission and knowledge of the holder. It is a form of cyber-attack with the main aim being theft of sensitive data to gain an advantage over a competitive company or government entity. It is an offence to gain access without authorization to gain critical data, database or critical national information.

It also provides for an offence of unauthorized interception. Any person who intentionally intercepts directly or indirectly and causes transmission of data to or from a computer system over a telecommunication system commits an offence. This aims at preventing people from intercepting communications on computer systems. The provisions under the Act provides

measures of data protection on computer systems. This is a crucial legislation for the 21st century especially due to the developing computer technology.

Kenya Information and Communications Act

This is the principle statute on matters of information and communication. It establishes the Communication Authority of Kenya that is the regulator in the communication industry.[114] It is the authority that grants licenses to providers of telecommunication. Section 5A establishes it as an independent authority to regulate the industry. This means that it is free from government control. Section 23 requires it to ensure provision of telecommunication services. In ensuring proper provision of telecommunication services, it is required to ensure that the services are of quality and fair price. In its role, it is also required to promote principles and values of the Constitution which includes human rights such as the right to privacy. Section 27 provides that the Minister in consultations with the Commission can make regulations with regards to privacy of telecommunications. These regulations are yet to be formulated.

Section 27A gives telecommunications provide an obligation to collect personal data of telecommunications providers. It is required to obtain one's personal full name, identity card number, date of birth, gender, physical and postal address. Section 27 (3) provides that these particulars for purposes of facilitating performance of any statutory functions of the authority, investigating of criminal offences or for civil proceedings. Failure to abide by the section is considered an offence and can attract a fine not exceeding five million.

Section 31 prohibits interception of communication by telecommunication providers. It also prohibits disclosure to any person on the message that has been intercepted. Section 83W prohibits interception of computer systems. Regulation 3 provides that consumers have the right

[114] Section 3, Kenya Information and Communications Act, 2013

to personal privacy. The provision also provides for protection from unauthorized use of personal information. Regulation 15 of the Kenya Information and Communications (Consumer Protection) Regulations (2010) prohibits telecommunications operators from disclosing contents of communications. Section 46A requires the Communications Authority to protect the right of privacy of all persons. Broadcasters are also required to respect the right of privacy of all persons.

The Communication Authority as stated above is an independent body that is required to uphold the right of privacy. This includes prevention of mass surveillance. In the case of Okiya Omtatah vs. Communication Authority of Kenya & 8 others[115] the government and the Authority was alleged to have contravened human rights including the right to privacy in the plans to introduce the Device Management System in the telecommunications industry. The device would enable government to monitor private communications therefore infringing on the right to privacy.

One of the issues that the court looked into was whether it violated or threatened the right to privacy and if it was in the affirmative, whether it met the requirements of Article 24 on the limitations of rights. The case handled issues on both data protection and the right to privacy. The interested parties in the case were telecommunications operators who felt that installing the system would go against their obligations as service provide to protect the privacy of their clients such as personal data. This was in furtherance to Section 27A(3) that obligated it to secure personal details of subscribers. The court held that the system was a breach to the right to privacy. The case is a good demonstration of the right to privacy and data protection with regards to government surveillance.

[115] [2018] eKLR

National Intelligence Service Act

The National Intelligence Service Act has been established under Article 242(1) of the Constitution of Kenya, 2010.The Constitution has established it as a body responsible for security intelligence and counter terrorism. The Act broadens these functions to include transmission of security intelligence, detection of threats to national security and promotion of national security. The Service is administered by the Director General.

Among the key principles guiding the service is complying with the standards of human rights. The Act provides on limitations of a number of fundamental rights and freedoms. Section 36 provides that the right to privacy can be limited for a person suspected of committing an offense. It provides for judicial oversight as it requires the National Intelligence Service to obtain a warrant before they can interfere with the one's communication. It allows interception of communications but restricts it to person suspected to have committed an offence. The Act does not allow the government to put up a mass surveillance system. Section 36 requires that right to privacy can only be limited on those persons that are under investigations.

The government has released the Draft National CCTV Policy for public participation.[116] The policy seeks to require public and private bodies to install CCTV (Closed Circuit Television) cameras.[117] These cameras will be required to be compatible with government digital security network. This creates room for mass surveillance.[118] Without proper regulation it can lead to infringement on the right to privacy.

[116] Amnesty International,' Kenya : Desist from Indiscriminate and Invasive Mass Surveillance,' < https://www.amnestykenya.org/wp-content/uploads/2019/08/Amnesty-International-Press-release-on-CCTV.pdf> accessed on 14th November 2019

[117] Ibid

[118] Ibid

Data Protection Act

The new law has borrowed heavily from the European General Data Protection Regulation. The Act grounds data protection under the right to privacy. Section 5 reiterates Article 31 of the Constitution by providing for the right to privacy of one's personal data. Coupled with Section 14, data processors are required to process that data without infringing on the data subject's right of privacy.

Section 2 of the Act defines personal data by laying out a list of what can be termed as personal data. This includes race, education, gender, fingerprints, contact details, correspondence religion, identifying number and among others. Comparing the form of definition adopted by the Act and the definition under the European's General Data Protection Regulations, Kenya's definition is far from being exhaustive. The General Data Protection Regulation defines personal data under Article 4 as any information relating to an identified or identifiable person. The gives a wider capture compared to the Kenyan one.

Another aspect to take note of is that the Act fully exempts a public body that is processing personal data that involves national security and in fighting crime. This is a highly strict approach considering that the GDPR allows member states to restrict the application of a number of articles on grounds of national security or fighting crime. These are provision such as data portability, rectification, transparency and accountability.

Section 7 requires that data should be collected for a specific reason. Data collectors are required to ensure that the data is complete, accurate and updated. Section 9 provides for the rights of a data subject. This includes right to be informed of the use of one's personal data, access to the data, correction of the data and deletion of misleading data. Section 11 requires that data

collectors fully notify themselves to the data subjects. The Act also requires them not to retain data for unreasonable time as laid out in Section 19.

Another aspect of the Act is that it recognizes property rights in personal data. The Act under Section 21 restricts data collectors from using personal data for commercial use. It requires a data processor to first seek the consent of the data subject and have a written contract on use of the data for commercial use.

The Act by fully exempting security or the crime prevention agencies makes data protection inadequate. Government surveillance operates under these agencies. The agencies process personal data of both criminals and non-criminals. Registration of persons in Kenya is under the Ministry of Interior Security which is also in charge of crime prevention agencies. Crime prevention organs should be required to have accountability and responsibility.

Conclusion

Protection of data protection is more on control and responsibility rather than restriction and prohibition.[119] The legal framework on data protection is inadequate. Kenya are also not protected in computer systems as many sections of the Computer Misuse and Cybercrimes Act remain suspended. The Data Protection Bill is still under debate in Parliament. Kenya requires a legal framework to sufficiently protect the right to privacy.

[119] Paul De Hert, Serge Gutwirth, David Wright & Gloria Gonzalez,' Legal Safeguards for Privacy and Data Protection in Ambient Intelligence,' (2008) Pers Ubiquit, page 442

CHAPTER THREE

NECCESSITY OF GOVERNMENT SURVEILLANCE

Introduction

The right of privacy includes both the right to be left alone and the right not to be monitored.[120] It is a sacred right that should be highly preserved.[121]Due to the growth of technology, state surveillance has immensely increased.[122] The state is at the position of large scale collection of personal data and communications.[123] The nature of government surveillance has widely grown especially with the emerging internet surveillance.[124] Internet surveillance has enabled government to intrude into private life therefore infringing on the right to privacy.

National security has been used by the government as a justification in infringing on the right to privacy.[125] It has made citizens to trade their privacy for security.[126] Although national security is a justification, governments usually fail to satisfy the principles of reason and proportionality in limiting human rights. Limitations of freedom and rights is justifiable in a democratic society. However, the state has to demonstrate that it has applied the limitation clause as required.

The balance between privacy and national security is becoming a hot discourse as digital technology advances and as levels of security threats grows.[127] This requires that there be a clear line between national and the right to privacy. The extent in interception by government must have clarity in law. Article 24 requires each interception to be justifiable and reasonable. The

[120] Daragh Murray & Pete Fussey,' Bulk Surveillance in the Digital Age: Rethinking the Human Right Law Approach to Bulk Monitoring of Communications Data,' (2019) 52 Israel Law Review, page 32
[121] Ibid
[122]Ibid
[123] Ibid
[124] Paul Bernal,' Data Gathering, Surveillance and Human Rights: Recasting the Debate,' (2016) 1 Journal of Cyber Policy, page 254
[125] Ibid
[126] Adam Moore,' Privacy, Security and Government Surveillance; WikiLeaks and the New Accountability,' (2011) Public Affairs Quarterly, page 141
[127] Betsey Casman, 'The Right to Privacy in Light of the Patriot Act and Social Contract Theory,' (2011) University of Nevada Professional Papers Journal, page 2

reasonability of limiting the rights and freedoms is in order to ensure that there is maintenance of peace and order. This has to be satisfied fully.

Reasonability, Proportionality and Necessity

Reasonableness was defined in the case of *R vs. Oakes*.[128] The court opined that limitation had to be sufficiently important in order to warrant overriding a right. The court stated that the standard had to be very high. This was in order to avoid reasons that were trivial and discordant. Justice Dickson stated that in each case of limitation of rights, there had to be a proportionality test. The test was for the court of law to balance the right of a society with those of a group. It further stated that the considerations must not be arbitral or irrational and the benefit that comes out of limitation had to be more that the detriment. This are the principles the court needs to scrutinize in balancing national security and privacy.

The right to privacy is founded on the premise of human dignity.[129] The right protects the self-respect of every human being. The government is the duty bearer and it has obligations to promote its realization other than infringing upon it. It is also arguable that since the government has a duty to protect people's right, it can infringe where it is justifiable especially in order to protect the right of others. There has been a heightened atmosphere for national security making governments to access and abuse personal information.[130] In jurisdictions such as USA, where the right to privacy and national security has been highly litigated, the right to privacy has been in most times been generally dismissed.[131] National security has in most times trumped the right

[128] (1986)
[129]
[130] Will Thomas, 'Protecting Privacy in the Digital Age,' (2003) 18 Berkeley Technology Law Journal, page 307
[131] Ibid

to privacy.[132] This has brought the view that more privacy results to less security and more security results to better security.[133] This has affected the need to balance privacy and security.

There is no legal framework that allows mass government surveillance in Kenya. This means that the national security organs have no legal capacity in intercepting private communications without a warrant. The surveillance can be conducted by the National Intelligence Service. There have been allegations on the Communication Commission of Kenya granting direct access to private communications. This allows the government to conduct bulk surveillance on Kenyan citizens. Bulk surveillance is a definite infringement of the right to privacy.[134]There have also been allegations of internet and social media monitoring. Direct access to private communications gives government unchecked powers which only results to infringement of the basic tenets of the right to privacy.

The government has the critical role of maintaining order and security and the citizens have fundamental rights and freedoms that are provided under the Constitution. Although there is need to protect human life, government surveillance has seriously affected privacy rights. This is especially with regards to bulk surveillance. There are three core concepts in matters of bulk surveillance.[135] One is the legal basis for it, two is its legitimacy and three is its proportionality and necessity in a democratic society.[136] This touches on when they occur and the balance with other competing rights.[137] The Constitution protects against mass surveillance. This determines

[132] Ken Himma,' Security and Liberty : The Image of Balance,' (2003) 11 Journal of Political Philosophy , page 13
[133] Ibid
[134] Eliza Watt,' The Right to Privacy and the Future of Mass Surveillance,' (2017) 21 International Journal of Human Rights, page 774
[135] Neil Richards,' The Dangers of Surveillance,' (1934) 126 Harvard Law Review, page 173
[136] Ibid
[137]

the cases when government surveillance can be said to have outweighed an individual's right to privacy.

Terrorism justifies interception of communications due to the threat it poses to lives of people. Mass surveillance in jurisdictions such as USA has been justified on the aspect that it is the best way in preventing terrorist attacks.[138] The absence of proper checks and balances leads to totalitarianism.[139] This allows unfettered surveillance that can easily lead to human rights abuse. It sacrifices privacy for security.

In the Kenyan case, we have the National Intelligence Service that is highly secretive. This means that surveillance is conducted in a highly secretive manner. This creates a threat of surveillance without judicial oversight. Government surveillance needs to be legitimate. Without legitimacy, human rights can easily be abused. Judicial oversight prevents speculative and abusive government intrusion.[140]This chapter seeks to bring a broad discussion on these analyses. It analyzes the surveillance in private and public spaces and also the impact of the surveillance on human rights.

As argued in chapter two, data protection goes beyond private spaces and captures other sectors that contain private data but are public in nature. This is especially corporates or the government itself holding private information. There are also public spaces such as the social media sites. Digital technology such as the social media have created records of personal life.[141]

[138] Emmanuel Boussios ,' The Right to Privacy? - The Debate over the United States Government's Control over its Cyberspace,' (2017) 2 Athens Journal of Law, page 222
[139] Ibid
[140] Mark Young, 'What Big Eyes and Ears You Have: A New Regime for Covert Government Surveillance,' (2001) 70 Fordham Law Review, page 1017
[141] Neil Richards,' The Dangers of Surveillance,' (2013) 124 Harvard Law Review, page 1934

Governments are intruding into the digital spaces to acquire personal data.[142] Technology surveillance has allowed governments to intrude in many aspects of private life.[143]

The major challenge with regard to surveillance is usually its scope.[144] A US Court in the case of *Katz vs. United States*[145] held that the right to privacy protected people and not places. It stated even users of a public payphone were protected from government interception. Judge Harlan gave a two part test in evaluating the right to privacy with regards to government surveillance. The first is that the person must have an expectation of privacy and two is that the society must recognize it as private.

Bulk surveillance has a great potential in undermining human rights. It has also been established that states such as USA and UK have been conducting surveillance beyond their borders.[146] This is challenging as there is no law that regulates foreign surveillance.[147] International law has not addressed matters of cross territorial surveillance and as a result it has led to spying and espionage. This can adversely affect international relations. The matters to be addressed in regulating cross-border surveillance are not different.[148] They are based on necessity and proportionality.[149]

Impact of Government Surveillance on Human Rights

Government surveillance can be harmful to human rights. One negative impact is that it can be used by government in order to find ways to curtail civil liberties such as freedom of expression.

---

[142] Ibid

[143] Jeffrey Childers, 'Kyllo vs. United States: A Temporary Reprieve from Technology- Enhanced Surveillance of the Home,' (2003) 81 North Carolina Law Review, page 728

[144] Omer Tene & Jules Polonetsky,' Big Data for All: Privacy and User Control in the Age of Analytics,' (2013) 11 North Western Journal of Technology & Intellectual Property,

[145] [1967] 388 U.S. at 353

[146] Asheley Deeks,' An International Legal Framework for Surveillance,' (2015) 55 Virginia Journal of International Law, page 292

[147] Ibid

[148] Marko Milanovic,' Human Rights Treaties and Foreign Surveillance : Privacy and Digital Age,' (2015) 56 Harvard International Law Journal, page 82

[149] Ibid

Through surveillance, the government can analyze the opinion of citizens from their communications. It can target those that give negative information on the government. This can also result to coercion and blackmail. This can make the citizens to shy away from expressing themselves. Surveillance in the digital spaces has been used by autocratic regimes such as China to monitor dissidents and this has highly limited the freedom of expression. Democratic states such as USA and Britain have also highly invested in surveillance technology in both private and public spaces.[150] Citizens need to be given the opportunity of intellectual freedom. This is the freedom to think on matters without state oversight.

The three arms of government play critical roles in government surveillance. The executive is the body that carries out the surveillance, the parliament enacts the necessary legislation and the judiciary provides oversight. The parliament is the biggest enabler of government surveillance as it provides the statutory capacity. This is especially by enabling secrecy in government operations in the name of national security. The law enforcement agencies are allowed to operate without disclosure if in their own interpretation, they view an issue as a matter of national security.

The judiciary's role is to provide oversight. It interprets the constitutionality of surveillance and decides if a surveillance is reasonable and necessary. The Kenyan government is a government of limited powers as it has been provided under Article 24.

The Kenyan court has dealt with two cases that touch on aspects of the right to privacy. One is the case of *Bloggers Association of Kenya (BAKE) vs. Attorney General & 5 Others*.[151] The case , which is still ongoing, is challenging provisions of the Computer Misuse and Cyber Crimes

[150] Brendan Palfreyman,' Lessons from British and American Approaches to Compelled Description,' (2009) Brook Law Review, page 362
[151] [2018] eKLR

Act. The court suspended provisions which the state argues were put to protect the right to privacy in computer systems. Another case is the case of *Nubian Rights Forum & 2 Others vs. the Attorney General & 8 others*.[152] The case challenged the collection of personal information by government. The court issued orders against the government from collecting DNA (Deoxyribonucleic Acid) information and Global Positioning System (GPS) data.

Apart from preventing intrusion or interception of private communication, the courts have a duty under Article 31 (a) and (b) of the Constitution to protect every person against search and seizure. The need for warrants is to ensure that there is reasonableness for the search and seizure. Section 118 of the Criminal Procedure Code require police to obtain search warrants from court. Police must prove on oath the necessity for a search. Section 25 provides for search of arrested persons and section 26 provides for search of vessels, vehicles and aircraft if there is believed that they have been used for a crime or stolen.

Role of Non- State Actors in prevention of Interception and Data Protection

Non state actors such as the telecommunications industry are big custodians of persona data and private communications. They are obligated to respect human rights.[153] As custodians of people private data and communications, they have an obligation to prevent intrusion and interception of private communications by the government.[154] Other industries have developed have made efforts to protect the privacy of their users by generating strong encryptions on their devices.[155] Law enforcement agencies across the globe have found it extremely hard to decrypt. This has

[152] [2019) eKLR
[153] Chris Jonick,' Confronting the Impunity of Non-State Actors: New Fields for the Promotion of Human Rights,' (1999) 21 Human Rights Quarterly, page 57
[154] Andrew Ungberg,' Protecting Through a Reasonable Decryption Policy,' (2009) 22 Harvard Journal of Law & Technology, page 541
[155] Ibid

contributed in protecting private data and preventing the government from intercepting in private communication.[156]

Recently, there has been a development of compelled decryption on corporates.[157] Industries such as phone industries , especially in jurisdictions such as USA are being forced by government to decrypt their devices for government to access data that is mostly private or confidential. Courts in USA have allowed government to compel companies to give it access even in fingerprint encrypted devices. A good case study on this is Apple and FBI (Federal Bureau of Investigations.[158] The case was taken in court and the FBI argued that it ought to be given access to information on the Apple product, iPhone. The court issued orders on Apple to put in a feature that could allow the FBI to hack the system. The court compromised on security and privacy.

Emerging legal framework such the General Data Protection Regulations have put more obligations on the data collectors and processors. Cases of mandated encryption have been on the increase especially in states with highly developed technology.[159] Corporates have put strong technology that are tough to decrypt making them to compel decryption by the service providers. Courts in USA have granted warrants to compel service providers to decrypt.[160] Decryption leads to more harm than good on the right to privacy.[161]

---

[156] A. Michael Froomkin,' The Metaphor is the Key: Cryptography, the Clipper Chip and the Constitution,' (1995)
[157] Aloni Cohen & Sunoo Park,' Compelled Decryption and the Fifth Amendment: Exploring the Technical Boundaries,' (2018) 32 Harvard Journal of Law & Technology, page 171
[158] Gus Hussein,' Compromising Over Technology, Security and Privacy,' (2017) 11 International Journal of Communication, page 907
[159] Scott Brady,' Keeping Secrets: A Constitutional Examination of Encryption Regulation in the United States and India,' 2012 22 Indiana International & Comparative Law Review, page 322
[160] Alohi Cohen & Sunoo Park,' Compelled Decryption and the Fifth Amendment: Exploring the Technical Boundaries,' (2018) 32 Harvard Journal of Law & Technology, page 171
[161] Andrew Ungberg,' Protecting Privacy Through a Responsible Decryption Policy,' (2009) Harvard Journal of Law & Technology, page 546

The non-state actors have the ethical duty to their clients to protect their personal data and communication. As the influence of non-state actors grow , their role in protection of human rights has widened.[162] The Constitution of Kenya, 2010 is the supreme law therefore they are obligated to protect the privacy of its clients even if it is the government unless the limitation of the right has met the threshold provided under Article 24.

Conclusion

Ensuring proper compliance in protection of privacy and its balance with national security is usually the major challenge. Government in most times violate the law and abuse people's rights. As government surveillance develops and with new technologies that promote surveillance and allow infringement of the right to privacy, there is need for law to address such matters. The technologies should not be misused as tools to infringe on people's rights. The government must disclose all the technology it intends to use on its citizens. This must be provided through statues. The court holds the biggest role in the protection of the right to privacy. It provides checks and balances on the executive. This aids in preventing abuse of power.

[162] Aoife Nolan,' Holding Non- State Actors to Account for Constitutional Economic and Social Rights Violations : Experiences and Lessons from South Africa and Ireland,' < https://www.researchgate.net/publication/275146833_Holding_non-state_actors_to_account_for_constitutional_economic_and_social_rights_violations_Experiences_and_lessons_from_South_Africa_and_Ireland> accessed on 16th August 2019

CHAPTER FOUR

COMPARATIVE ANALYSIS

Introduction

The Right to privacy varies from state to state. Due to rapid technological growth across the globe, the right to privacy has become exposed to abuse. Technological advancement has led to increase in surveillance of private space, interception of private communication and intrusion on personal data. This has made states to put laws such as data protection to aid in securing people's privacy.

Data protection has emerged to secure the right to privacy. The EU is widely viewed as the best framework for data protection. This is especially because other states outside Europe such as South Africa has used the EU's framework in formulating their domestic statute for data protection. The Global Data Protection Regulation (GDPR) has become the global best practise for data protection law.

In this chapter, three jurisdictions have been selected. These are USA, European Union and South Africa. USA has been selected as it is a jurisdiction where the right to privacy has been widely discussed together with the aspect of national security. Both USA and Kenya face terror threats which prompt government to put surveillance systems. USA is among the top jurisdictions that have wide laws on government surveillance. Its laws on data protection have also developed immensely. Europe is regarded as the best global practise due to the Global Data Protection Regulation. Its data protection laws is wide capturing data protection rights and also matters of national security. South Africa is a study as it is an African developing state and has just formulated laws on data protection. It is a good benchmark for Kenya.

USA

The Fourth Amendment protects the rights to privacy by providing the right against searches and seizures. Data protection is yet to be recognized as a separate and distinct right. The balance of national security and the right to privacy is a contentious issue in USA. It has a Presidential Surveillance programme that monitors its citizens.

The US supreme court addressed the issue of government surveillance touching on technological development. This was in the case of *Kyllo vs. United States*.[163] In the case of *Olmstead vs United States* the court interpreted the constitutionality of wiretapping. The court held that wiretapping was constitutional. It held that as long as there was no invasion of a suspect's premises, one's right to privacy had not been violated.

Surveillance has highly developed due to the growth of sophisticated devices.[164] The law enforcement organs have used wiretaps which has enabled them to surveil private communications and also used the same as evidence before court.[165] Organs such as Central Intelligence Agency (CIA) ,Drug Enforcement Agency (DEA) and Federal Bureau of Investigations (FBI) have developed sophisticated surveillance technologies. Technological-assisted surveillance is seen as an essential tool for law enforcement organs in

The government has also used private sector players for surveillance. This includes telephone companies and even banks. Through the Communications for Law Enforcement Act of 1994, private companies especially telephone companies have been compelled in enabling law enforcement organs to intercept on private communications. Private citizens are also used for

[163] [2000] 121 S. Ct. 2038

[164]

[165] Mark Young, 'What Big Eyes and Ears You Have: A New Regime for Covert Government Surveillance,' (2001) 70 Fordham Law Review, page 1017

government surveillance. The court in the case of *USA vs White*[166] held that there was no need for warrant if a private citizen voluntarily decided to wear a wire when speaking with the law enforcement agency's target.

Government surveillance through use of wiretaps is statutory provided through the Omnibus Crime Control and Safe Streets Act of 1968. The Act was enacted to provide a balance between protecting the right to privacy and promoting effective law enforcement. The Act prohibits wiretapping except for the law enforcement agencies. Before the law enforcement agencies can carry out a wiretap on telephone communication, the Act requires that an official of high rank in the Attorney General's office to make an application to a federal judge or magistrate. The official is required to prove commission of a crime or a crime is about to be committed, that the particular communication will be used for commission of a crime, type of interception on the communication and that there is no other means or that other means have failed. Another Act is the Electronic Communication Privacy Act of 1986. The Act was enacted to capture other forms apart from telephone. This was foe emails and voice mail. There are other statutes with provisions on government surveillance. One is the Foreign Service Intelligence Act of 1978. The Act allowed interceptions for national security purposes.

Apart from statutes that provide for surveillance, they are statutes that provide for the right to privacy. These includes the Video Privacy Act, Privacy Protection Act and the Federal Privacy Act. The Cybersecurity Information Sharing Contract Act and Cyber Intelligence Protection Act have put obligations on officials of the law enforcement agencies on data protection. There is the Health Insurance Portability and Accountability Act of 1996 that requires information on health of persons to be protected.

[166] [1971] US 745

After the terrorist attack, USA enacted the Patriot Act. The Act was enacted to aid in fighting terrorism. The Act increased government surveillance immensely. It allowed government to conduct surveillance on suspicion of terrorism. It allowed for surveillance on internet communications. It provided for exchange of information on surveillance between law enforcement agencies. It limited the right to privacy for national security. It. The Act gave the government access to data held by private entities. It could acquire private information held by employers.

European Union

European Union was the first international instrument to recognize the right to data protection [167] This was through the Lisbon Treaty which was enacted in the year 2009.[168] Data protection has advanced in Europe due to the recognition of data protection as a standalone fundamental right and freedom.[169] Other international instruments such as the International Covenant on Civil and Political Rights have not recognized data protection as a distinct human right. Its regulations on data protection is stricter compared to USA.[170] It has put stricter sanction on infringement of data privacy.[171] Its law prohibit processing of personal data unless it meets the legal basis.

The Charter of Fundamental Rights of the European Union provides for the right to data protection under Article 8. Article 8 provides the elements of data protection. It provides that every person has the right to have their personal data protected. The provision requires that personal data has to be processed fairly and should be for a specified purpose. The consent of the

[167] Yvonne McDermott,' Conceptualizing the Right to Data Protection in the Era of Big Data,' (2017) Big Data and Society, page 1
[168] Ibid
[169] Paul Schwartz,' The EU –US Privacy Collission : A Turn to Institutions and Procedures,' (2013) 126 Harvard Law Review, page 1967
[170] Ioanna Tourkorchoriti,' The Transatlantic Flow of Data and the National Security Exception in the European Data Privacy Regulation: In Search for Legal Protection Against Surveillance,' (2015) 36 U.Pa.J.Int. L. , page 460
[171] Ibid

person must be sought and the person must have the right to access the information and have to corrected in case of any error. The same provision also provides that there should be an independent regulator. The provision creates obligation on each person to protect private data. The obligation to protect this right has been put on any organization that collects private data. Protection of private data is also provided under Article 16 of the Treaty of the Functioning of the European Union.

Europe has the strongest standards and enforcement on data protection due to it recognizing data protection as a distinct right.[172] Many of the EU states have regulations on data protection.[173] In Spain and Germany, it imposes huge fines on those that violate the data privacy laws. The regulations mostly target the private actors. It does not apply to matters that concern national security. Its application is highly limited in matters of law enforcement agencies and national security.

In most of the EU states, the data protection laws do not protect against government surveillance. It prevents surveillance by the private entities. The European Court has determined a number of cases on the issue of government surveillance. One is on the case of *Klass vs. Germany*.[174] In this case the applicants brought a case against the government when they formulated a secret surveillance program in its statute. They argued that this was an infringement on the right to privacy. The court stated that surveillance was allowed under the Convention as long as it was necessary for the protection of domestic institutions. It went further to state that the surveillance should be in accordance to law.

[172] Nooraneda Laidey, 'Privacy vs. National Security: Where Do We Draw the Line? '(2015) 9 International Scholarly and Scientific Research & Innovation, page 2235
[173] Ibid
[174] [1978]

In UK, the Investigatory Powers Act 2016 provides the legal basis for government surveillance. For surveillance of communication, it requires that the law enforcement agency to look at the extent of information, extent of harm, and its utility to the law enforcement organs. Cases of mass surveillance have been subject to litigation.

The EU framework for data protection began with the EU Data Protection directive of 1995. The directive aided the member states in coming up with legislation for data protection. They were developed from Article 8 of the Convention of Fundamental Right and Freedoms of the EU. The growth of technology and computer systems led to a different approach. This led to the formulation of the General Data Protection Regulation by the European commission. The first draft was published in 2012. It came into effect in 2018.

The Global Data Protection Regulation (GDPR) is the principal framework for data protection. The framework provides for a number of aspects on the right to privacy. It is one of the instruments under EU with heavy penalties for non- compliance. Organizations that abuse the right to data protection can be fined based on their turn over to a tune of 4%.

One of the aspects is the need for consent when obtaining private data. Under Article 7, it requires that the consent to collect personal information be intelligible, clear, in a plain language and accessible to the person. It requires that collection of personal information to be non-discriminative. The collection exercise should not be for profiling. This is provided under Article 9.

Under Article 5 and 6 deals with processing of personal data. Article 5 provides the data protection principles. It requires processing of data to be fair, lawful and transparent. Data processors are required to demonstrate their compliance with the principles. Article 6 provides

that any agreement that allows the data controller to derogate from data quality is invalid from the onset. This also applies to those contracts that prevent access rights of the owner of the data. It guides processing of personal data. It requires the data to be processed in a transparent manner. The collection is required to be for a specified purpose and necessary. Where data is wrongly entered, it requires rectification. Chapter three provides for right of persons in data protection. This includes the right of access to the information under Article 13. This applies even through the data was obtained from another source apart from the data subject as provided under Article 14. Article 16 provides for the right to be forgotten, this is a right where one can require an entity to erase all the personal information they have.. Article 25 and 26 provide for regulation in dissemination of personal data to third parties.

Article 23 provides the limitations on data protection and privacy. This is in a number of instances including for national security, defense, public security, judicial independence. Article 25 puts obligations on the one collecting personal information on safeguarding the information. Article 33 requires the person to report on any breach to the supervisory authority. The data controller of processor is required to notify the supervisor within 72 hours. They are required under Article 34 to notify especially where the breach would lead to breach of human rights.

The regulations recognize the effect of technology on private data especially on collection and dissemination. Article 35 provides for data protection impact assessment for new technologies. This is for instances where there is a new technology. The purpose is to test the technology to ensure that it does not infringe on the rights of its users.

Article 82 allows one to seek compensation in court if his or her right to data protection has been abused. If one suffers material or non-material damage he can seek damages from the data processor. One can also lodge a complaint to the supervisory authority as provided under Article

77. The supervisory authority has been given wide powers in safeguarding the right to privacy. Article 78 allows one to seek judicial remedy where the supervisory authority has failed to make a decision.

South Africa

The right to privacy is protected in the Constitution of South Africa. The provision is not different compared to the Kenyan provision. The right is also not an absolute right. The principal statutes that provides for the right to data protection is the Protection of Personal Information Act, 2013. The Act provides wide measures on processing of personal information. It requires consent be granted in processing of sensitive information. It requires that all data processors to be accountable, collect only specific information, put up security safeguards and provide access to the data subjects. Data processors are prohibited from sharing data with third parties in other countries unless the data subject has given consent, transfer is necessary for performance of a contract or its conclusion with the data subject.

Section 19 of the Act puts ide obligation on the data processors. It requires them to put up measures to protect personal data. The data processor is required identify the foreseeable internal and external risks, put up appropriate safeguards for those risks and constantly update them. Section 22 requires the data processor to notify the Information Regulator. The notification must be made as soon as possible.

Conclusion

Kenya has formulated a law on data protection. However, the legal framework must recognize and borrow from global best practise. This will aid in ensuring that Kenya has established a proper framework. The provisions in the Data Protection Bill are heavily borrowed from the EU jurisdiction. This will aid in securing personal data. However, the bill has exempted public agencies that process personal data for national security and criminal investigation. Although

limiting data protection on the basis of national security and crime prevention is justified, it ought to be regulated to a reasonable extent rather than being fully exempted.

CHAPTER FIVE

CONCLUSION AND RECCOMENDATIONS

Introduction

The four chapters have discussed on the aspect of finding a balance between the right to privacy and national security. This has been evaluated especially with regards to the growth of the right to data protection as an emerging right. The lack of a proper legal framework on data protection has highly affected the right to privacy. Kenya's legal framework on data protection has been fragmented and this has not provided proper protection. This has prompted legal reforms hence the introduction of the Data Protection Bill, 2018 at the Senate. To secure personal information in this age of big data, data protection laws have been seen to be of necessity.

The first chapter introduced the problem for the thesis. It covered the aspects that were to be discussed in the thesis. The second chapter analyzed the constitutional and statutory provisions. The third chapter looked deeply into the question of national security with regards to right to privacy. The fourth made a comparative analysis with other jurisdiction. Below is the conclusion and recommendations that this research has arrived at.

Conclusion

The study has established that though there are constitutional and statutory basis for limitations of the right to privacy, there are a number of grey areas in its regulation. The study looked into the aspect of national security and government surveillance. It determined that there is inadequate framework for judicial oversight on surveillance. It established that there were inadequate data protection laws to protect personal information from intrusion by both state and

non-state organs. The Data Protection Bill seeks to cover a lot of the loopholes in law. However, it is too general with regards to limitations on the ground of national security. The Bill under Clause 3 exempts the provisions of the bill's application on processing of personal data by a public body for national security or prevention of crime. The provision is too general and gives the government unlimited power when it collects personal data through surveillance. This is because through government surveillance, government may collect personal data not related to national security or commission of crime. This information should be deleted.

The study established that data protection is not synonymous with the right to privacy but it is an emerging right that has developed in order to promote the right to privacy in the current age of big data. Under the Kenyan Constitution, the right to data protection is not explicit but emerges from Article 31(c) that requires one's personal information from being unnecessary required or revealed. This touches on the aspect of control and transmission of personal data which is a major element in the right to data protection. However, the current law does not adequately provide for data protection.

The Data Protection Bill has borrowed a lot of its provisions from the EU's Global Data Protection Regulation. The bill has good provisions that will protect personal information. However, while the bill has provided wide measures on private bodies, it has not covered public bodies adequately. This is amid the many reports that have been given showing that the Kenyan government has been conducting surveillance on its citizens.

There is need to have better regulation on the limitation of the right to data protection on the ground of national security. This is especially with regards to government surveillance. The Bill is still vague as it exempts processing of personal data by public bodies. More judicial oversight needs to be put up in order to ensure that Kenyans are better protected.

The statutes that allow government intrusion to privacy are very general and do not meet constitutional necessity. They lack adequate provisions on disclosure and judicial oversight. In judicial oversight, it does not require the government to disclose on the form of surveillance or interception. It only requires that the surveillance be on a specified person. Judicial oversight is limited to the initial phase and not the process whereby personal that is not related to national security may be collected while collecting the relevant data.

The current law and the bill does not adequately safeguard the right to be forgotten. The right of one to seek deletion of personal information is restricted under clause 9 of the Data Protection Bill to misleading information or objected. EU's General Data Protection Regulations has widely expanded this right to personal data that is no longer necessary to the person who collected the information and where consent has been withdrawn, the data was unlawfully processed.

Recommendations

The court in its judicial oversight in government surveillance should require the law enforcement agencies to be accountable and disclose the form of technology it is using for surveillance. This is in order for the court to ensure that the form of surveillance, although focused on a particular person, does not give room for mass surveillance.

The Parliament should come up with legislation that restricts the forms of technology that are used for surveillance. There should be a proper legislation to incorporate accountability, transparency and adequate oversight of surveillance systems to ensure that the government does not infringe on privacy of innocent individuals in the process of investigations of criminal suspects.

The courts should strictly evaluate every application by law enforcement agencies for surveillance or search and seizures. It should scrutinize the purpose and ensure that it meets the constitutional threshold.

Legislation should address the risk new technologies have posed on privacy. The Computer Misuse and Cybercrimes Act addressed some of the threats that have been brought by the new technology. There are other such as personal tracking.

Non- states actors such as corporate should take more responsibility in promoting the right to privacy. They should not release personal data to any person and also to government without seeking consent or court order. Corporates should also take proper measures such as modern form of encryption to ensure that personal information is not easily accessed by third parties.

Strict sanctions should be put on government officials, corporates or any other organization that shares personal data to third parties without the consent of the owners.

Mass surveillance should be viewed as unconstitutional and any form of surveillance that promotes indiscriminate access to private data should well regulated or personal data protected. New technological advances such as government surveillance tools such as camera should be regulated to ensure third party access is highly restricted and it is not used to target communities. For instance, USA has been constantly accused of using its surveillance tools to monitor the Muslim community.

Due to technological advancement, surveillance is beyond telecommunication channels. The Prevention of Terrorism Act is restricted to telecommunications channels. It does not protect one from interception of one's online activities and electronic devices such as computer.

BIBLIOGRAPHY

Books

1. Dirk Voorhoof,' Freedom of Expression versus Privacy and the Right to Reputation,' in Stijn & Eva Brems, *When Human Rights Clash at the European Court of Human Rights: Conflict of Harmony?* (Oxford University Press, 2017)
2. Johaness Morsink,' *Inherent Rights : Philosophical Roots of Universal Declaration*,' (2012) University of Pennsylvania Press
3. Evangelia Psychogiopoulou & Maja Brkan Courts, *Privacy and Data Protection in The Digital Environment in the Digital Environment* (1st Edition, Edward Elgar Publishing Limited
4. G.G Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (1ST Edition, Springer 2004)
5. Orla Lynskey, *The Foundations of EU Data Protection Law*, (1st Edition, Oxford University Press, 2015),

Articles

1. Adam Moore,' Privacy, Security and Government Surveillance; WikiLeaks and the New Accountability,' (2011) Public Affairs Quarterly
2. Aloni Cohen & Sunoo Park,' Compelled Decryption and the Fifth Amendment: Exploring the Technical Boundaries,' (2018) 32 Harvard Journal of Law & Technology
3. Andrew Ungberg,' Protecting Through a Reasonable Decryption Policy,' (2009) 22 Harvard Journal of Law & Technology,
4. Andrew Serwin,' Privacy 3.0-The Principle of Proportionality,' (2009) 42 University of Michigan Law Journal

5. Alex Makulilo,' Privacy and Data Protection in Africa: A State of the Art,' (2012) 2 International Data Privacy
6. Asaf Lubin, 'We Only Spy of Foreigners : The Myth of a Universal Right to Privacy and the Practise of Foreign Mass Surveillance,'(2018) 18 Chicago Journal of International Law
7. Asheley Deeks,' An International Legal Framework for Surveillance,' (2015) 55 Virginia Journal of International Law
8. Ashok Kumar, 'Surveillance and Right to Privacy :Issues and Challenges,' (2017) 3 International Journal of Law
9. Betsey Casman, 'The Right to Privacy in Light of the Patriot Act and Social Contract Theory,' (2011) University of Nevada Professional Papers Journal
10. Brendan Palfreyman,' Lessons from British and American Approaches to Compelled Description,' (2009) Brook Law Review
11. Craig Konnoth, 'The Expressive Theory of Privacy Intrusions,'(2017) 102 Iowa Law Review
12. Chris Jonick,' Confronting the Impunity of Non-State Actors: New Fields for the Promotion of Human Rights,' (1999) 21 Human Rights Quarterly
13. Carol Nackenoff,' Privacy, Police Power, and the Growth of Power in the Early Twentieth Century : A Not So Unlikely Coexistence,'(2015) 75 Maryland Law Review,
14. Daniel Marcus,' The Data Breach Dilemma: Proactive Solutions for Protecting Consumers' Personal Information,' (2018) 68 Duke Law Journal
15. Daniel Solove, 'Conceptualizing Privacy,'(2002) 90 California Law Review

16. Daniel Solove,' The Taxonomy of Privacy,'(2006) 154 University of Pennsylvania Law Review
17. Dennis Hirsch, 'Privacy, Public Goods, and the Tragedy of the Trust Commons :A Response to Professors Fairfield and Engel,'(2016) 65 Duke Law Journal
18. Dorothy Glancy, 'The Invention of the Right to Privacy,'(1979) 21 Arizona Law Review David Flaherty,' On the Utility of Constitutional Rights to Privacy and Data Protection,'(1991) 41 Case Western Law Review,
19. Daragh Murray & Pete Fussey,' Bulk Surveillance in the Digital Age: Rethinking the Human Right Law Approach to Bulk Monitoring of Communications Data,' (2019) 52 Israel Law Review
20. Eliza Watt, 'The Right to Privacy and the Future of Mass Surveillance,'(2016) 21 International Journal of Human Rights
21. Emmanuel Boussios ,' The Right to Privacy? - The Debate over the United States Government's Control over its Cyberspace,' (2017) 2 Athens Journal of Law
22. Gerald Cope ,'Toward a Right of Privacy as a Matter of State Constitutional Law,'(2014) 5 Florida State University Law Review
23. Gunter Frankenberg,' Human Rights and the Belief in a Jus World,' (2014) 12 Oxford University Journal
24. Gus Hussein,' Compromising Over Technology, Security and Privacy,' (2017) 11 International Journal of Communication
25. Fred Cate, Christopher Kunner, Christopher Millard & Dan Jerker ,'The (Data Privacy) Law Hasn't Even Checked in When Technology Takes Off,'(2014) Articles by Maurier Faculty

26. Hannah Yee Fen, ‘The Data Protection Paradigm for the Tort of Privacy in the Age of Big Data,’(2015) 27 Singapore Academy of Law Journal,
27. Ioanna Tourkochoriti,’ The Transatlantic Flow of Data and The National Security Exception in the European Data Privacy Regulation: In Search for Legal Protection Against Surveillance,’ (2015)
28. James Griffin,’ The Human Right to Privacy,’ (2007) 44 San Diego Law Review
29. Juliane Kokott & Christophe Sobotta,’ The Distinction Between Privacy and Data Protection in the Jurisprudence of the CJEU and the EctHR,’ (2013) 3 International Data Privacy Law
30. Jed Rubenfeld, ’The Right to Privacy,’(19890 102 Harvard Law Review
31. Jeffrey Childers, ’Kyllo vs. United States: A Temporary Reprieve from Technology-Enhanced Surveillance of the Home,’ (2003) 81 North Carolina Law Review
32. Jody Ferris,’ Data Privacy and Protection in the Agriculture Industry :Is Federal Regulation Necessary?,’(2017) 18 Minnesota Journal of Law, Science & Technology
33. Joshua Fairfield & Christoph Engel ,’Privacy as a Public Good,’(2015) 65 Duke Law Journal
34. Jonathan Manes, ‘Online Service Providers and Surveillance Law,’(2016) 125 Yale Law Journal
35. Jose Alvarez,’ The Human Right to Property, ‘University of Miami Law Review
36. Ken Himma,’ Security and Liberty : The Image of Balance,’ (2003) 11 Journal of Political Philosophy
37. Kamal Hossain,’ Methods of Dealing with Violations of Human Rights: What Needs to be Done and Why it is Not Done,’ (1982) 9 Yale Journal of International Law

38. Kathleen Paisley,' It Is All About Data: The Impact of the EU General Data Protection Regulation on International Arbitration,'(2018) 41 Fordham International Law Journal
39. Kriangsak Kittichaisaree & Christopher Kuner,' The Growing Importance of Data Protection in Public International Law,' (2015) European Journal of International Law
40. LA Bygrave,' Data Protection Pursuant to the Right to Privacy in Human Rights Treaties, (1998) 6 International Journal of Law and Information Technology
41. Luciano Florida,' On Human Dignity as a Foundation for the Right to Privacy,' (2016) Philosophy & Technology Journal
42. Lyn Entrikin, 'The Right to Be Let Alone: The Kansas Right of Privacy,' (2014) 53 Washburn Law Journal
43. Maria Tzanou, 'Data Protection as a Fundamental Right Next to Privacy? Reconstructing a Not So New Right,' (2013) 3 International Data Privacy Law
44. Mark Young, 'What Big Eyes and Ears You Have: A New Regime for Covert Government Surveillance,' (2001) 70 Fordham Law Review
45. Marko Milanovic,' Human Rights Treaties and Foreign Surveillance : Privacy and Digital Age,' (2015) 56 Harvard International Law Journal
46. Major Harding, Mark Criser & Michael Ufferman,' Right to be let Alone? Has Adoption of Article 1 , Section 23 in the Florida Constitution , which Explicitly Provides For a State Right to Privacy, Resulted in Greater Privacy Protection for Florida Citizens?,'(2014) Notre Dame Journal of Law, Ethics & Public Policy
47. Menno Mostert, Annelin Bredenoord, Bart van der Sloot & Johannes van Delden,' From Privacy to Data Protection in the EU: Implications for Big Data Health Research,' (2017) 24 European Journal of Health Law

48. Napoleon Xantholis,' The Right to Oblivion in the Information Age: A Human-Rights Based Approach,' (2013) 10 US-China Law Review
49. Naomi Arriaza,' State Responsibility to Investigate and Prosecute Grave Human Rights Violations in International Law,' (1990) 78 California Law Review
50. Natasha Mavriocola,' What is an Absolute Right? Deciphering Absoluteness in the Context of Article 3 of the European Convention on Human Rights,'(2012)12 Human Rights Law Review
51. Neil Richards,' The Dangers of Surveillance,' (1934) 126 Harvard Law Review
52. Omer Tene & Jules Polonetsky,' Big Data for All: Privacy and User Control in the Age of Analytics,' (2013) 11 North Western Journal of Technology & Intellectual Property
53. Paul Bernal,' Data Gathering, Surveillance and Human Rights: Recasting the Debate,' (2016) 1 Journal of Cyber Policy
54. Samuel Warren & Louis Brandies,' The Right to Privacy ,'(1890) 4 Harvard Law Review
55. Sylvia Kierkegaard,' Privacy in Electronic Communication: Watch your Email, Your Boss is Snooping,' (2005) 21 Computer Law & Security Review
56. Smith Grinell & Rabin Colette,' Modern Education : A Tragedy of Commons,' (2013) 45 Journal of Curriculum Studies
57. Stefan Schuster, Melle Berg, Tom Slewe & Peter Kostic,' Mass Surveillance and Technological Policy Options : Improving Security of Private Communications,' (2017) Computer Standards & Interfaces
58. Spiros Simitis, 'Privacy- An Endless Debate?' (2010) California Law Review

59. Scott Brady,' Keeping Secrets: A Constitutional Examination of Encryption Regulation in the United States and India,' 2012 22 Indiana International & Comparative Law Review
60. Teraya Koji,' Emerging Hierarchy in International Human Rights and Beyond: From the Perspective of Non Derogable Rights,' (2001) 12 European Journal of International Law
61. Thomas Emerson,' The Right of Privacy and Freedom of the Press,' (1979) 14 Harvard Civil Rights-Civil Liberties Review,
62. Rachel Waldman ,'Government Access to and Manipulation of Social Media :Legal and Policy Challenges,'(2018) 61 Harvard Law Journal
63. Richard Bruyer,' Privacy : a Review and Critique of the Literature,'(2006) 43 Alberta Law Review
64. Will Thomas, 'Protecting Privacy in Digital Age,' (2003) 18 Berkeley Technology Law Journal

Internet Sources

1. Aoife Nolan,' Holding Non- State Actors to Account for Constitutional Economic and Social Rights : Experiences and Lessons from South Africa and Ireland,' < https://www.researchgate.net/publication/275146833_Holding_non-state_actors_to_account_for_constitutional_economic_and_social_rights_violations_Experiences_and_lessons_from_South_Africa_and_Ireland> accessed on 16th August 2019
2. Consumers International, 'The State of Data Protection Rules Around the World: A Briefing for Consumer Organizations,' <

https://www.consumersinternational.org/media/155133/gdpr-briefing.pdf > accessed on 17th May 2019

3. Privacy International,' Track , Capture , Kill : Inside Communication Surveillance and Counterterrorism in Kenya,' < https://privacyinternational.org/sites/default/files/2017-10/track_capture_final.pdf>
4. Yvonne McDermott,' Conceptualizing the Right to Data Protection in an Era of Big Data,' < https://journals. sagepub. com/doi/pdf/10.1177/2053951716686994 > accessed on 20th May 2017

Thesis

1. Patrick Odhiambo,' Limitation of Rights under the Kenyan Constitution,' (LLM Thesis, University of Pretoria, 2015