THE RIGHT TO PRIVACY IN KENYA

UNIVERSITY OF NAIROBI

ABIDHA NICHOLUS OWINO PETER

G62/82428/2015

A research project submitted in partial fulfilment of the requirements for the award of degree of Master of Laws (LLM) of the University of Nairobi

December, 2019

DECLARATION

I, **Abidha Nicholus Owino Peter**, do hereby declare that this is my original work and that it has not been submitted for award of a degree or any other academic credits in any other university.

Abidha Nicholus Owino Peter

G62/82428/2015

Signed …… Date…….

This research project has been submitted for examination with my approval as a University supervisor.

Signed …… Date…….

Dr. Deputy Chief Justice (Rtd) Nancy Baraza

DEDICATION

I dedicate this project to Mama Wilikista Onang'o Ondolo alias Nyogony, my loving Grandmother, who always reminded me of how she terminated her education prematurely due to her unconditional obedience to her mother. Indeed, I promised to carry the baton from where she left to the highest possible level. I also wish to dedicate this project to my late Mum who, during her lifetime, encouraged me to pursue my dreams with passion.

ACKNOWLEDGEMENT

I acknowledge support and assistance of Hon. Deputy Chief Justice (Rtd.) Dr. Nancy Baraza who has guided me throughout this project. She set apart time from her busy schedule, including weekends and public holidays, to peruse my drafts and make invaluable comments and recommendations.

I appreciate the support of my Grandmother, Dani Wilikista Nyogony, who cherishes education so much and for her prayers.

I also acknowledge support of Oliver Abidha and Akinyi Abidha, who have accorded me invaluable care and support during the long duration I took to put this together. Besides, members of Abidha & Company Advocates managed to create a favourable environment for me to conclude this project and I remain indebted to them.

TABLE OF CASES

TABLE OF LEGISLATION

Conventions, treaties, protocols and regulations

African Charter on Broadcasting, 2001

African Charter on Human and Peoples' Rights, 1981

African Charter on the Rights and Welfare of the Child, 1990

African Declaration on Internet Rights and Freedoms, 2013

African Platform on Access to Information Declaration, 2011

African Union Convention on Cyber-security and Personal Data Protection, 2014

American Convention on Human Rights, 1969

ASEAN Human Rights Declaration, 2009

Asia-Pacific Economic Cooperation Privacy Framework,2005

Convention on Rights of the Child, 1989

Convention on the Organization for Economic Co-operation and Development, 1960

Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 1981

Council of Europe Recommendation No. R(99) 5 for the Protection of Privacy on the Internet

Data Protection Directive (Directive 95/46/EC

Declaration of Principles on Freedom of Expression in Africa, 2002

Kenya

HIV and AIDS Prevention and Control Act, No. 14 of 2006.

Kenya Information and Communications Act (KICA) Chapter 411 A Laws of Kenya (Revised in 2015).

National Intelligence Service (NIS) Act, 2012.

Official Secrets Act, Chapter 187 of Laws of Kenya.

Children's Act, Chapter 141 Laws of Kenya.

Penal Code, Chapter 63 of Laws of Kenya.

Private Security Regulation Act, No. 13 of 2016.

Public Archives and Documentation Service Act, Chapter 19 Laws of Kenya.

The Security Laws (Amendment) Act (2014).

The Prevention of Terrorism Act (2012).

Witness Protection Act No. 16 of 2006.

Banking Act, Chapter 488 Laws of Kenya.

South Africa

Constitution of the Republic of South Africa, 1996.

Electronic Communications and Transactions Act 25 of 2002(ECTA).

Protection of Personal Information Act 4 of 2013 ("POPI").

Regulation of Interception of Communications and Provision of Communications Related Information Act (RICA) (2002).

Bills

Cyber security and Protection Bill, 2016.

Data Protection Bill, 2015.

Data Protection Bill, 2018 by the Senate of Kenya.

Data Protection Bill, 2018 by the Ministry of Information, Communications & Technology

Data Protection Bill, 2019 by National Assembly of Kenya.

Kenya Information and Communication (Amendment) Bill 2019.

Policy Papers

Data Protection Policy, 2018.

National Information and Communication Technology Policy, 2016.

Kenya National Vision 2030.

ACRONYMS

CAK	Communications Authority of Kenya
FTC	Federal Trade Commission
EC	European Commission
ECHR	European Convention of Human Rights
EU	European Union
GUID	Globally Unique Identifier
ICT	Information Technology
ICCPR	International Covenant on Civil and Political Rights
IP	Internet Protocol
OECD	The Organization for Economic Co-operation and Development
PII	personally identifiable information
SEACOM	Undersea cables
SNS	Social Networking Sites
TEAMS	The East African Marine System
UDHR	Universal Declaration of Human Rights
UK	United Kingdom
UN	United Nations
URL	Uniform Resource Locator
USA	United States of America

DEFINITION OF TERMS

Anonymised/Pseudonymised data	data that does not allow that a person can be identified
Computer	means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, software and communication facilities which are connected or related as a system or network;
Cookies	a block of text code-digital identification tags- which the website places in a file on a computer hard disk of a person to track his activity.
Critical infrastructure	means vital virtual systems and assets whose incapacity or destruction would have a debilitating impact on the security, economy, public health and safety of the country;
Cyber	of, relating to, or involving computers or computer networks (as the Internet.
Cybersecurity threat	means an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is store;

Data processing	converting of data into information. This includes collecting, recording, rationalizing, storage, alteration, retrieval, use, transmission, dissemination, erasure or destruction of data;
Data controller	a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of processing of personal data;
Data processor	a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller;
Data subject	an identified or identifiable natural person who is the subject of personal data;
Encryption	the process of converting the content of any readable data using technical means into coded form;
E-mail or document bugs	reports time and date the email or message is opened.
Globally unique identifier-	is software that is embedded in computer software.
Internet Protocol address	personally identifiable information that is automatically captured by another computer when any communications link is made over the internet.
Internet	a means of connecting a computer to any other computer anywhere in the world via dedicated routers and servers.
Online digital profiling-	various companies have advertisements on web pages tagged with cookies which once clicked start building up the user's profile as he moves from one site to another.

Online	being accessible via a computer or computer network
Privacy	the state or condition of being free from being observed or disturbed by other people.
Sensitive personal data	Data that reveals sensitive personal traits such as genetics, biometrics, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health status or sex life/ sexual orientation;
Social networking service also social networking site	is a platform to build social networks or social relations among people who share similar interests, activities, backgrounds or real-life connections.
Spyware	these are codes that cause user's computer to transmit information back to the software developer via internet.
Technology	the application of scientific knowledge for practical purposes, especially in industry.
Web bugs	is part of a banner advertisement on a website's web page that a person is viewing which causes a person's browser to transmit to the advertiser's server, the URL of the page the person is visiting.
WWW	Worldwide Web

TABLE OF CONTENTS

ABSTRACT

History has shown that the right to privacy has developed into a fundamental human right. This is manifested in both international laws and domestic Constitutions of various states. Kenya in particular has enshrined right to privacy, which incorporates data protection, under Article 31 of the Constitution, 2010.

The right to privacy is the foundation of other rights and freedoms hence it is not an absolute right. This study argues that the extent of enjoyment of that right and limitations can only be demarcated through an Act of parliament. Unfortunately, such legislation was lacking in Kenya until the enactment of Data Protection Act, 2019 thus crippling the full realization of right to privacy as envisaged under Article 31 both offline and online.[1] There are different statues on protection of diverse aspects of privacy in Kenya but the same are inadequate because they fail to address the challenges brought about by technological developments and extensive online activities amongst Kenyans.

This study examines the foundation of right to privacy in Kenya and further assesses the paradigm shift occasioned by promulgation of the Constitution, 2010 specifically on right to privacy. It reviews some of the provisions of the existing legislation and finds that they inadequately tackle the modern challenges, threats and risks to privacy both offline and online therefore limiting the enjoyment of the right to privacy.

The study further draws lessons from other jurisdictions like Ghana, South Africa and European Union on modern legislation and regulations focused on protecting privacy in digital and online

1 The Data Protection Act, No. 24 of 2019

platforms and recommends the same to Kenya in its quests to enact a legislation to enable realization of Article 31 of the Constitution, 2010.

CHAPTER ONE

1.0 Introduction

This study examines relevant materials on the right to privacy with focus on laws of Kenya. It identifies the gaps in the legal regime of Kenya which hinder the full enjoyment of right to privacy as envisaged in the Constitution of Kenya by examining the origin, history and development of right to privacy and examines its impact on net users in Kenya. It further interrogates the development of protection of privacy in line with progress made in Europe while at the same time compares the legal regimes of right to Privacy in Kenya with that of South Africa and Ghana then proposes raft of reforms to enable full realization of the enjoyment of privacy as envisaged in the Constitution of Kenya.

1.1 Background

The protection of privacy has been perceived and defined variously by different scholars and practitioners mostly depending on various circumstances and jurisdictions. Thus, the impression created so far is one without a refined single definition of privacy. The fresh challenge has been introduced by rapid technological development and ease of access to information through the internet specifically worldwide web.

Judge Cooley opined that the right to privacy is the right to be alone without any unwarranted interference or intrusion.[2] On the other hand others believed that the right to privacy accorded each individual the powers to determine the extent of how, why and when his thoughts,

2 Thomas Cooley, A treatise on the law of torts, or the wrongs which arise independent of contract 2ed (1888) Chicago, Callaghan & Co.

sentiments and emotions can be accessed by others.[3] On this backdrop, it was argued that the right to privacy had in it four torts *to wit* intrusion upon the plaintiff's seclusion or solitude or into his private affairs,[4] public disclosure of embarrassing private facts about the plaintiff,[5] publicity which places the plaintiff in a false light in the public eye[6] and appropriation of a person's name or likeness.[7] Other Scholars view protection of privacy as a right of an individual to control collection, use and disclosure of his personal data and that it is the basis of other freedoms of association, movement and life.[8]

The 21st Century scholars conceive the right to privacy by importing heavily from the traditional definitions. Shyamkrishna defines, the right to privacy to encompass collection, retention, use and disclosure of information[9] the same being viewed as the ability of an individual to control personal information and determination if, when and how the same is obtained and utilized.[10]

Privacy has been protected in Kenya as it was one of the rights under the repealed Constitution.[11] It focused more on protection of intrusion of homes and other physical spaces and properties but not informational privacy.

The Constitution of Kenya 2010, on the other hand has offered a broad and liberal perspective to this right hence providing for protection of privacy of person, home, property and communication

3 Samuel Warren and Louis Brandeis, 'Right to Privacy' (Harvard Law Review(1890)

4 William Prosser, 'Privacy' (1960) 48 California Law Review 384

5 Ibid

6 Ibid

7 Ibid

8 Stephen Sedley, 'Towards a Right to Privacy,'(2006) London Review of Books

9 Shyamkrishna BalGanesh and Neelanjan Mitra, 'Cryptography, Privacy and National Security Concerns', Law Relating to Computers, Internet & E-commerce' (5th Edition Universal Law Publishing Co Pvt Ltd 2013)

10 Arthur Robertson, Privacy and Human Rights (1st Edition, Manchester University Press 1973).

11 Constitution of Kenya 1969 (now repealed) s.70 (c) which provided that:

Protection for the privacy of his home and other property and from deprivation of property without compensation.

be it of their family members or themselves.[12] This is closely related to South African foundation of privacy which protects person, home, property and communication albeit limited to the individual.[13]

It is notable from the two provisions the Kenyan Constitution[14] guarantees wider right to privacy than the South African version.[15] This is a clear departure from legal regime of right to privacy which existed prior to 2010 which was very limited in its scope. In addition, there is a Constitutional obligation on all public and private actors to respect all rights and fundamental freedoms including protection of privacy and related rights.[16]

Besides, the scope of the constitutional protection of privacy in Kenya is also wider than the duty of confidentiality under the principles of common law. Thus, by protecting privacy in communications it guarantees right to privacy in online networking sites where research has shown rising number of users.[17] This broad clause can be said to have envisioned various technological developments, availability of devices and ease of access to the internet prompted by affordable costs. The greatest boost of the protection of privacy under the Kenyan Constitution is the applicability of International laws and principles including best practices.[18]

The international law guarantees the protection of privacy and related rights under United Nations Universal Declaration of Human Rights,[19] International Convention on Civil and

12 Constitution of Kenya, 2010 Art. 31

13 Constitution of the Republic of South Africa, 1996, Art14

14 Ibid n12, Art 31

15 Ibid n13

16 Ibid n12 Arts 19 and 20

17 Ibid n12 Art 31(d)

18 Ibid n12 Art 2(5) & (6)

19 United Nations Universal Declaration of Human Rights Art 12

Political Rights 1966,[20] United Nations Convention on Migrant Workers[21] and the UN Convention on the Rights of the Child.[22] Indeed, the Human Rights Committee demanded that member states should take legislative measures on protection of privacy and related rights.[23]

The United Nations resolved and affirmed that the protection of privacy online based on emerging technologies must be of equal standard as that offered offline.[24] It called upon the member states to ensure protection of privacy and related rights by having oversight mechanism founded in law and impartial in its decision making to take appropriate measures against public agencies and private entities including individuals to prohibit surveillance of communications, their interception and the unauthorized collection of personal data. [25]

At the continental level, Europe has various advanced instruments meant to protect privacy and related rights including Convention for the Protection of Human Rights and Fundamental Freedoms,[26] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data,[27] Data Protection Directive,[28] and Data Protection Regulation **(**GDPR)[29] which repealed Data Protection Directive.[30]

---

20 Ibid Art 17

21 Ibid Art14

22 Ibid Art16

23 General Comment No. 16 Article 17

24 http://undocs.org/A/RES/68/167 101 Resolution 69/166, UN General Assembly. http://dag.un.org/bitstream/handle/11176/158167/A_RES_69_166-EN.pdf?sequence=3&isAllowed=y; Human Rights Council, The Right to Privacy in the Digital Age. https://bit.ly/2xDfKAx; Summary of the Human Rights Council panel discussion on the right to privacy in the digital age, Report of the Office of the United Nations High Commissioner for Human Rights http://www.un.org/en/ga/search/view_doc.asp?symbol=A/HRC/28/39; Text of the Convention, https://rm.coe.int/1680078b37 accessed on 08/09/2019

25 Ibid

26 Article 8 available at https://www.echr.coe.int/Documents/Convention_ENG.pdf

27 ETS No. 108 available at https://rm.coe.int/1680078b37 accessed on 25/11/2019; Council of Europe Recommendation No. R(99) 527 for the protection of privacy on the Internet

28 European Union Data Directive Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data available at http://www.europarl.europa.eu/ftu/pdf/en/FTU_4.2.8.pdf

29 Directive 2016/679

Pundits have decried the legislative framework on protection of privacy and related rights in the United States of America observing that apart from American Convention on Human Rights[31] it merely rely on patchwork of sectoral laws of privacy protection while it houses some of the companies in data economy and techno-business with worldwide coverage advanced thereby exposing the net users to online risks and dangers.[32] In Asia, privacy is protected under Asia-Pacific Economic Cooperation Privacy Framework[33] and Human Rights Declaration of the Association of Southeast Asian Nations.[34]

In Africa, privacy and related rights are protected under the Platform on Access to Information Declaration of 2011,[35] Declaration of Principles on Freedom of Expression in Africa,[36] African Charter on Human and Peoples' Rights,[37] Charter on Broadcasting,[38] Windhoek Declaration on Promoting an Independent and Pluralistic African Press,[39] African Union Convention on Cyber-security and Personal Data Protection of 2014[40] together with Personal Data Protection Guidelines for Africa[41] and Charter on the Rights and Welfare of the Child.[42]

In addition, various organizations concerned with internet regulation developed the African Declaration on Internet Rights and Freedoms with the intention to address some of the challenges

---

30 Directive (Directive 95/46/EC)

31 http://www.cidh.org/Basicos/English/Basic3.American%20Convention.htm

32 https://www.cfr.org/report/reforming-us-approach-data-protection accessed on 08/09/2019

33 https://www.apec.org/Publications/2005/12/APEC-Privacy-Framework

34Art. 21 available at https://asean.org/asean-human-rights-declaration/

35 Adopted at the Pan African Conference on Access to Information (PACAI) on 19 September 2011

36 Resolution 350 (ACHPR/Res.350 (EXT.OS/XX) 2016 available on https://www.achpr.org/public/Document/file/English/draft_declaration_of_principles_on_freedom_of_expression_in_africa_eng.pdf

37 http://www.humanrights.se/wp-content/uploads/2012/01/African-Charter-on-Human-and-Peoples-Rights.pdf

38 Published on 18/12/2001

39 Endorsed by the General Conference at its twenty sixth session - 1991

40 https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

41 https://www.internetsociety.org/wp-content/uploads/2018/05/AUCPrivacyGuidelines_2018508_EN.pdf

42 https://www.unicef.org/esaro/African_Charter_articles_in_full.pdf

bedeviling internet usage and users including protection of privacy and related rights in online platforms.[43]

Better understanding of the protection of privacy and related rights online is only possible on evaluation of the origin of the right to privacy, its scope and development. Further, examination of the variations brought about by the development in technology is paramount. This will help in understanding whether the constant developments of technology have been incorporated in the existing laws.

1.2. Statement of problem

Lack of specific legislation on privacy has hindered full realization of protection of privacy and related rights as envisaged under the Constitution of Kenya.[44] This right is linked and subject to other rights and freedoms enshrined in the Constitution thus its enjoyment is limited. Therefore, an enabling statute was expected to provide for both platform for enjoyment of the right together with various limitations based on international laws and best practices. Thus, in the absence of the enabling statute the Courts have continued to apply principles applicable in other jurisdictions and limitations of other rights and freedoms which might not be apt for full enjoyment of protection privacy and related rights.

1.3. Theoretical framework

The right to privacy touches on the autonomy, dignity and esteem of a person. It forms the foundation of other fundamental rights including but not limited to expression, movement, life

43 https://africaninternetrights.org/ accessed on 18/10/2019

44 Ibid n12 Art 31

and consciousness.[45] This highlights the issue of morality in law which this paper examined to establish if right to privacy is premised on public or private morality. In both instances and taking into consideration the emerging technologies, it is worth addressing the need to regulate private morality. This argument intends to disapprove the position that it is not business of the law to regulate the realm of private morality[46] which is shared by H.L.A Hart.[47] The research adopts the views of Devlin to the extent that law makers legislate on morals.[48]

This paper expounds on Devlin's concept of morality as a basis of law. It demonstrates that both the urge to protect privacy and requirement for regulation is not only an imposition of the law makers' will but the compulsion and pressure from the users of such networks both to protect themselves as individuals to attain not only self-determination but also autonomy in decision making.

The relevance of the theory and concept of morality in laws run through the entire research from assessment of the origin of right to privacy, developments in light of modern technologies, the emergence of online privacy and its misuse/abuse and the hypothesis that there is need for regulation of social network sites in Kenya.

Privacy is a right inherent in all human beings exercisable in all places at all times hence fitting well within Simmons conceptions of human rights to the extent that such rights are moral rights; any person possesses this right at all times and in all places simply by virtue of being human and the duty bearers on the other hand must protect and respect this right in appropriate

45 Camrin L. Crisci, 'All the world is not a stage: Finding a right to privacy in existing and proposed legislation (2002) 2 N.Y.U Journal of Legislation and Public Policy, 215

46 Wolfenden Report of the Committee on Homosexual Offences and Prostitution (1957)

47 H.L.A Hart, Essays in Jurisprudence and Philosophy (1983).

48 P. Devlin, The Enforcement of Morals (Oxford: University Press, 1959)

circumstances.[49] The human rights conception of right to privacy will be evident in discussing privacy as a foundation of other rights, its limitations and universal nature.

1.4. Literature Review

1.4.1. The Origin of Right to Privacy

Privacy has been protected from time immemorial as captured in religious books.[50] Different communities and societies also have privacy but the seriousness and intensity of its protection differ from one place to another.[51] The oldest attempts to recognize privacy as an enforceable right is traceable from America around 1492 which ushered its application to correspondence, person, property[52] and even decisions.[53] The Courts also enforced this right in various instances and even awarded damages.[54]

Warren and Brandeis[55] later urged that there was need to address privacy as an enforceable right to encourage intrusion into private spheres of individuals.[56] But the Courts were not in consensus about the enforcement of privacy as aright.[57] Thereafter, the confirmation of privacy as a right by the Court was only prompted by public outcry which seemed to have propped the position taken

49 John Simmons, Justification and Legitimacy, (1999), 109, No. 4 Ethics 739

50 Will DeVries, Protecting Privacy in the Digital Age (2003) 18 Berkeley Technology Journal 283. The Holy Bible and Qu'ran.

51 Dominic Dagbanja, Privacy in context: the right to privacy, and freedom and independence of the media under the Constitution of Ghana

52 Daniel Solove, 'A Brief History of Information Privacy Law' [2006] GW Law Faculty Publications & Other Works 1.

53 Blackstone William, Commentaries on the Laws of England, (1769) Clarendon Press at Oxford 168

54 De May V. Roberts, 46 Mich. 160, 9 N.W. 146 (1881). The Court held that: It would be shocking to our sense of right, justice and propriety to doubt even but that for such an act the law would afford an ample remedy. To the plaintiff the occasion was a most sacred one and no one had a right to intrude unless invited or because of some real and pressing necessity.

55 Warren and Brandeis (n1)

56 Prosser (n4).

57 Prosser (n4).

by Warren and Brandeis.[58] However, the Courts in America in attempting to adjudicate on violations of privacy failed to develop clear principles and opted for common law principles.[59]

Based on the foregoing it is clear that protection of privacy predated the views of Warren and Brandeis and lack of decisive definition ought not to be viewed as an impediment to realization of benefits and protections of this right.[60] It is evident that most of scholars can describe it albeit variedly due to various factors in different societies.[61]

1.4.2 Scope of the Right to Privacy

The protection of privacy and related rights envisage the presumption that human beings are entitled to autonomy in their liberty, space, development and various private aspects of life.[62] This is considered as "private sphere"[63] with others or in solitude free from interruption and interference by both the public and private entities or individuals the sovereignty of an individual.[64] The scope of protection of privacy is understood by zoning the right itself, having noted the self-determination of an individual. [65] This right also covers decisions on persons, property or family which an individual makes based on the autonomy inherent in him.

58 Pavesich v. New England Life Insurance Co.,15 122 Ga. 190, 50 S.E. 68 (1905). The Court held that: One who desires to live a life of partial seclusion has a right to choose the times, places, and manner in which and at which he will submit himself to the public gaze. Subject to the limitation above referred to, the body of a person cannot be put on exhibition at any time or at any place without his consent. . . It therefore follows from what has been said that a violation of the right of privacy is a direct invasion of a legal right of the individual.

59 Prosser (n4).

60 Ann Cavoukian, 'Privacy by Design' 2010 - Identity in the Information Society 3 (2):247

61 Britz J. J., Technology as A Threat To Privacy: Ethical Challenges to the Information Profession, University of Pretoria available at http://web.simmons.edu/~chen/nit/NIT'96/96-025-Britz.html accessed on 26/11/2019

62 Ibid

63 National Coalition for Gay and Lesbian Equality and Another v Minister of Justice and Others (CCT 11/98) [1998] ZACC 15.

64 Ibid.n38

65 Informational self-determination- the power of an individual to reveal personal data. as defined by Dr. Ann Cavoukian Go Beyond Security- Build in Privacy, at <http:/www.eff.org/pub/Privacy accessed on 05/09/2019

Such zone of privacy covers both autonomy in making certain kinds of important decisions and a person's interest in refusing disclosure of personal matters.[66] Other related aspects include financial privacy, foreign surveillance, employees and medical amongst others.[67] Family, person, correspondence and intimate decisions[68] are considered as core of privacy under the traditional human rights approach.[69] The foregoing is underpinned by the environment of space one needs for growth, development and self-discovery together with expectation that such environment is guaranteed under the law.[70]

Protection of privacy and related rights is a key component of the public interest as it is geared towards the protection of the integrity, esteem and autonomy of an individual[71]. However, it must be exercised within the broad spectra subject to freedom of expression, thought and beliefs which must be balanced so as to achieve public interest.[72] But such restrictions must be exercised in line with the law.[73] Privacy is actionable per se but it is personal and cannot be assigned and no claim can accrue upon death of the victim.[74]

66 Ibid

67 Supra (n26)

68 Universal Declaration of Human Rights available in https://www.ohchr.org/en/udhr/documents/udhr_translations/eng.pdf

69 Stephen Whittle and Glenda Cooper, 'Privacy, Probity and Public Interest' Reuters Institute for the Study of Journalism University of Oxford, 2008.

70 ibid

71 The law now affords protection to information in respect of which there is a reasonable expectation of privacy, even in circumstances where there is no pre-existing relationship giving rise of itself to an enforceable duty of confidence. That is because the law is concerned to prevent the violation of a citizen's autonomy, dignity and self-esteem. It is not simply a matter of 'unaccountable' judges running amok.(Mosley v News Group (July 2008), para. 7. The entire judgment can be found at http://news.bbc.co.uk/1/shared/bsp/hi/pdfs/24_07_08mosleyvnewsgroup.pdf)

72 ibid (n17)

73 Abdul Noorani, 'The Right to Privacy' (2005) 40 Economic and Political Weekly 802.

74 Supra (n 3).

It is confirmed that privacy exists as a distinct right and its unlawful invasion has liability and consequential remedies to the victim founded on both international and domestic laws.[75] But it is subject to limitation of public security, health, security or morality together with boundaries of rights and freedoms of others.[76] However, such restrictions must be fair, just and reasonable and based on would be allowed in a democratic society.[77]

Privacy is the exercise of autonomy by an individual to determine when, how and to what extent third parties access them or their personal information.[78]Freedom of information impacts on privacy and related rights like data protection because it regulates flow of information and access to official information even though the same are protections against certain aspects of abuse.[79]

The above analysis shows that privacy is the power of the individual to make decision on what people could know about him. This is because it is the foundation of enjoying other basic rights including right to life amongst others. Hence it is proper to conclude that in the absence of esteem, autonomy and integrity an individual's life could be miserable or even worthless. However, this argument may not hold in light of the changes that have occurred from 17th century up to date. We therefore examine various developments concerning right to privacy and its impacts.

1.4.3 Developments in Right to Privacy

Historically, privacy was viewed from the perspective of oppressive governments that violated the rights of individuals and groups which led to the international organizations formulating

75 Sharma Vakul, 'Offence-Breach of Confidentiality and Privacy', Information Technology Law and Practice, Law & Emerging Technology Cyber Law & -Commerce (4th Edition, Universal Law Publishing Co Pvt Ltd 2007).

76 Ibid.

77 Supra (n49).

78 A. Westin, 'Privacy and Freedom', Privacy and Freedom (Bodley Head 1970).

79 Chris Reed, 'Electrronic Privacy and Access to Information', Computer Law (7th Edition, Oxford University Press Inc 20`11).

instruments such as Universal Declaration of Human Rights and European Convention of Human Rights focused on the protection of people's fundamental rights which also guaranteed protection of privacy.[80] However, such instruments were formulated with the foresight on the strengths of individuals and corporations to the extent that privacy is enforceable against individuals and legal persons in what has been called horizontal application. This application has been described as realignment in light of its departure from focusing on restricting state power to positive standards of human conduct.[81]

The protection of privacy which was guaranteed in 17th to 19th Century still subsists, for instance protection of privacy is accorded to homes, children, sex, medical, financial, family life, personal correspondences and private documents.[82] However, this is negated by desire of some people to expose their lives intentionally[83] otherwise known as voluntary disclosure, accidentally or ignorantly using the modern avenues like the internet and other modes of communication.[84]

The advanced technological devices for instance the internet, micro cameras and mobile phone cameras have rapidly changed and even enhanced how we could invade our own privacy—or that of others. For instance consider information available on various online platforms which have a pool of personal identifiable information which is available to large number of people who also share the same thereby exposing such information to unexpected quarters.[85] The law on right to

80 Equality and Human Rights Commission, What is the European Convention on Rights, available on https://www.equalityhumanrights.com/en/what-european-convention-human-rights

81 ibid.

82 Roy Moore and Michael Murray, 'Right of Privacy', Media Law and Ethics (4th Edition, Routledge 2012).

83 Ibid (n 34).

84 Thomson Judith, 'The Right to Privacy' (1975) 4 Philosophy and Public Affairs 295.

85 Ibid (n 43). p.11:' Privacy has been commoditized. On the one hand individuals now have the possibility to profit from the manipulation of their privacy—whether by allowing it to be displayed in carefully organized and packaged slices, as celebrities of all kinds do; or by offering it up on the altar of the public gaze, as those wishing to be famous, or only to 'connect', as Big Brother demonstrates.

privacy has developed to cover emerging technological advances including telephone interception, wiretapping, bugging, computers and other modes of communication and data collection and storage called for development of law on right to privacy.[86]

These devices, in as much as they have improved and enhanced interaction between human beings they remain the greatest threats to privacy as argued above.[87] In addition, the web has been converted into many things including a playroom and people create both fact and fiction around their persona which ends up shared by others endlessly.[88] People therefore invent, exaggerate and openly communicate fake impressions which they share with others. This has made the web so enticing to the extent that it is difficult for people to refrain from sharing data online which they would otherwise not share offline.[89]

Google[90] and other search engines have information on what people search for online with the possibility that if such information is divulged then people's private lives could be restricted.[91]
Ian Walden argues that in the modern world intangible information is an asset and that a substantial portion of such information is personal data which reveal personal data to third parties hence breaching protection of privacy.[92]

Such personal information could be invaluable and thus need for legal regime to protect the same while maintaining the delicate balance of the interests of third parties, their security, health, safety

86 Fredric Karr, 'What Is Privacy? How the Law Translates to the Human Experience' (1996) 23 American Bar Association, Human Rights 9.

87 Supra n68

88 Ibid

89 Ibid

90 Google Inc,., 'Privacy Policy (2018)'.

91 S Knight, 'All-Seeing Google Street View Provokes Privacy Fears', The Times, 1 June 2007': <http://technology.timesonline.co.uk/tol/news/tech_and_web/article1870995.ece>. accessed on 07/05/2019

92 Chris Reed, 'Electrronic Privacy and Access to Information', Computer Law (7th Edition, Oxford University Press Inc 20`11).

and businesses.[93] The protection of personal data may be achieved by laws on intellectual property, trespass and interception of communication amongst other regimes.[94] But the biggest challenge that is notable from the above arguments is the threats by individuals to themselves by voluntarily disclosing intimate information to third parties without caring whether the same falls in the wrong hands.[95]

English Courts developed a cause of action, known as tort of misuse of private information which required on to prove that he had reasonable expectation of protection of private data and that the same was threatened with unauthorized disclosure.[96] The test of a reasonable person with sensibilities was applied and balanced with established public interest to come up with proportionate decision.[97] Once non-disclosure was justified an injunction against disclosure would issue.[98]

1.4.4 Privacy and data protection

Data protection is predominantly a European phenomenon recognized a distinct legislative field mainly focused on controlling the processing of automated personal data.[99] On the other hand, developing states suggest that data protection encompass the protection of information pertaining to the public which include information and knowledge affecting sovereignty, security, economic, morality or health of the public.[100]

93 David Smolin, 'The Jurisprudence of Privacy in Splintered Supreme Court' (1992) 75:975 Marquett Law Review 975.

94 Ibid n92

95 Parent W. A., A New Definition of Privacy for the Law, Law and Philosophy, Vol. 2, No. 3 (Dec., 1983), pp. 305-338

96 Campbell vs Mirror Group Newspapers Co Ltd (2004) 2 World Law Rep 1232; (House of Lords).

97 Thomson Judith, 'The Right to Privacy' (1975) 4 Philosophy and Public Affairs 295.

98 Ibid

99 Supra n92

100 Marie Baezner and Patrice Robin, Trend Analysis: Cyber Sovereignty and Data Sovereignty, 2018, Center for Security Studies (CSS), Zurich – Switzerland.

In the United Kingdom the jurisprudence has distinguished protection of privacy and data to the extent that the former is engaged *ex post*, once the abuse arises, while the latter is *ex ante* mechanisms to regulate control and processing of both public and private pieces of information.[101] Other distinctions have also been made in terms of enforcement thus whereas an individual presents before a court an issue of breach of privacy, data protection is advanced by regulatory authority in establishing compliance on the part of an agency charged with processing personal data.[102]

Kenya has the constitutional foundation of privacy which covers prohibits acts of intrusion into solitude, correspondence, family information and those affecting private data in possession of various entities.[103]

1.4.5 Privacy and technology

Technology equips a person to safeguard his privacy while at the same time exposes such a person to others' scrutiny. However, authors are divided about protection of privacy in the technology driven world with some indicating that it is a mirage[104] while others are optimistic that such rights exists and ought to be protected.[105]

The anti-privacy protection argue that a user of online medium can always be tracked both at the time of use and thereafter. Digital footprints they argue are traced by capturing the Internet Protocol (IP) address and as such he is making informed choice of plunging into the dangerous

101 Campbell vs Mirror Group Newspapers Co Ltd (2004) 2 World Law Rep 1232

102 Juliane Kokott and Christoph Sobotta, The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR, International Data Privacy Law, Volume 3, Issue 4, November 2013, Pages 222–228

103 Constitution, 2010, Art.31

104 Michael Froomkin, 'The Death of Privacy' (2000) 52 Stanford Law Review 1461.

105 Supra (n 49).

territory knowing consequences very well.[106]Generally Technology has provided platform for development of software and applications which are both useful and harmful because some of them have been used to surreptitiously violate privacy and protected data in ways that the victims.[107]Some users subscribe to the applications and software without full knowledge about the extent to which they collect private data and share the same.

1.4.6 Right to Privacy and International Law

International treaties and conventions guarantee the protection of privacy of every individual under the United Nations Universal Declaration of Human Rights,[108] International Convention on Civil and Political Rights, 1966,[109]United Nations Convention on Migrant Workers[110] and the UN Convention on the Rights of the Child.[111]

All these instruments provide for protection privacy and related rights and envisage the horizontal enforcement of the same thus demanding that different jurisdiction to enact legislation to guarantee full realization and protection of this right.

The Organization for Economic Co-operation and Development (OECD) has been praised for recognition of right to privacy way back in 1980 when its Council made recommendations[112] resulting into Guidelines Governing the Protection of Privacy and Transborder Flows of

106 personally identifiable information that is automatically captured by another computer when any communications link is made over the internet. Whenever a person browses, visits a site, sends an email or chats online, he leaves his distinct IP address behind which can be searched either through IP registration databases or by conducting a trace route, to determine an approximate physical location of an IP address.

107 Privacy International, 'The Right to Privacy in the Digital Age'(2018)

108 Ibid Art 12

109 Ibid Art 17

110 Ibid Art 14

111 Ibid Art 16

112 based on articles 1(c), 3(a) and 5(b) of the Convention on the Organization for Economic Co-operation and Development Paris 14/12/1960 https://www.oecd.org/general/conventionontheorganisationforeconomicco-operationanddevelopment.htm

Personal Data.[113] The said principles recognized protection of privacy and related rights as a human right.[114] It also harmonized various member states' legislation on trans-border data processing and sharing which is the hallmark of protection of privacy.[115]

In 2013 the Council revised the Recommendations to make them robust and alive to the current challenges.[116] It enhanced accountability in flow of data amongst member states inter se and with third parties based on the principle of free flow and legitimate restrictions.[117]

The foregoing international instruments make sense only if the protection of privacy is understood in terms of the modern interactions of various people globally. This is because technology has created global village to the extent that transactions and correspondent between individuals in different corners of the world are able to transact and communicate in real time.[118] Consequently, large amounts of data of personal nature cross national boarders either through internet or manual transfer of media (hard-disk and note book computers) and personal digital assistants.[119] This has been enhanced by the development of the internet into a market like platform which has facilitated emergence of speedy means of communication.[120] This clearly exposes the need to have laws and regulations geared towards protecting personal data taking into account the challenges of data havens, development of technology and voluntary breaches.

113 [C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79] available on https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf

114 Ibid

115 Fred Carte, Peter Cullen & Viktor Mayer-Schönberger, Data Protection Principles for the 21st Century Revising the 1980 OECD Guidelines, 2014.

116 https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf accessed on 03/07/2019

117 OECD Guidelines Governing The Protection Of Privacy And Transborder Flows Of Personal Data , 2013 page 13 available at https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf accessed on 13/04/2019

118 Ibid n9

119 Camrin L. Crisci, 'All the world is not a stage: Finding a right to privacy in existing and proposed legislation (2002) 2 N.Y.U Journal of Legislation and Public Policy, 215

120 Ibid n50

1.4.7 Right to Privacy in Kenya

The Constitution of Kenya guarantees the protection of right to privacy albeit substantive legislation to operationalize that provision took time to be enacted and is yet to be operationalized.[121]However, it is notable the Constitution imports international best practices and the use of international conventions, treaties and recommendations thus the Kenyan Courts could apply and be guided by the precedents in other countries and other good practices.[122]

Laws of Kenya allow the authority in charge of communications to collect data about individuals with a potential that the same might be shared with third parties notwithstanding that the Act prohibits such disclosures.[123] Further, there are steps taken by Kenya to secure privacy and personal data, albeit the same have been actualized but yet to be operationalized, including Data Protection Bills, Draft Data Protection Policy of 2018 and Data Protection Act.[124]

1.5 Objectives of the study

1.5.1 Main Objective

To assess the foundation of the right to privacy in Kenya in light of the guarantee in the Constitution, 2010.

1.5.2 Specific Objectives

The specific objectives of the study are to:

a) To analyze the legal regime on right to privacy in Kenya;

121 Data Protection Act, 2019

122 Privacy International and National Commission on Human Rights, 'The Right to Privacy in Kenya'.

123 Kenya Information and Communications Act. Chapter 411 A Laws of Kenya (Revised in 2015) allowing Communications Authority to access certain aspects of private communications

124 Kenya ICT Action Network, Policy Brief, Data Protection in Kenya, 2018 available at https://www.kictanet.or.ke/?wpdmpro=data-protection-in-kenya accessed on 12/10/2019.

b) To identify the gaps in the legal regime of right to privacy in Kenya both offline and online; and

c) To propose reforms on legal regime on right to privacy in Kenya.

1.6 Justification/significance of the study

The Constitution of Kenya guarantees the right to privacy which imposes prohibition on breach of privacy of person, home or property from being searched, seizure of possessions; unnecessary demand or disclosure of information relating to family or private affairs and infringement of the privacy of communications.[125]

Besides, the Constitution enjoins both state and non-state actors to respect rights and freedoms, privacy being one of them.[126] In addition the general rules of international law and any treaty or convention ratified by Kenya form part of the law of Kenya pursuant to Article 2(5) and (6) of the Constitution. However, this right is limitable and subject to other rights and freedoms.[127] This therefore calls for enabling legislation to define the confines of the right to privacy as envisaged in the Constitution. Notably, since the promulgation of the Constitution in 2010 Kenya took 9 years to enact the enabling legislation which is yet to be operationalized notwithstanding the emerging issues of privacy emanating from technological and online developments.

This study will analyse the legal regime on protection of privacy in Kenya with a view to understanding whether lack of specific legislation on right to privacy is a hindrance of full realization of the benefits envisaged under the Constitution more particularly in online platforms.

125 Ibid n12 Art 31

126 Ibid n12 Arts 2, 19, 20 and 21

127 Ibid n12 Art 24 and 25

The recommendations flowing from this research are geared towards formulation of the enabling legislation to realize full enjoyment of right to privacy more particularly online users.

1.7 Hypotheses

a) Privacy in Kenya is protected under the Constitution, 2010 and international law.

b) There is no specific legislation in operation to guarantee the full enjoyment of the right to privacy as envisaged in the Constitution which also affects net users.

c) There is need to propose reforms to realize the full enjoyment of protection of privacy and related rights as envisaged in the Constitution, 2010.

1.8 Research questions

1. What is the foundation of the right to privacy in Kenya?
2. Does Kenya have specific laws on protection of privacy and data?
3. What reforms will achieve full realization of enjoyment of right to privacy offline and online.

1.9 Methodology

The methodology provides a description of the procedures that will be followed in conducting the research. It describes the research site, study design, sampling techniques and procedure, and methods of data collection and analysis and, lastly, ethical considerations.

This project is based on both primary and secondary sources of data. The author endeavored to conduct interview and sample data on the core issues of this research. The author used the sample questionnaire attached at the end of this paper. The information collected was analyzed and

presented as part of conclusions/recommendation. In addition, the author analyzed legislation, cases, policy paper, reports and various pieces of literature which have formed the substantial portion of this research.

The identified secondary sources are in the form of books, articles and journals by reknown authors in the relevant fields which are available in of and hard copies in libraries and online. The sources include judicial decisions, published books, journals, papers, periodicals, authoritative published works, Government documents/reports, media sources and the internet.

The study will also compare the legal regime on privacy in Kenya and other foreign jurisdictions including Ghana, South Africa and Europe which have progressive laws on protection of privacy and data.

1.10 Ethical considerations

The research relates to issues which touch on people's private information and may also be in respect to some confidential government information. Such materials will be discussed but without disclosing information that could be contrary to individual's right to privacy, public security, morality and interest. These pieces of information will be sourced from judicial decisions of both Kenya and other jurisdictions.

1.11 Scope of the study

This study focuses on privacy offline and online within the parameters of Kenyan law. However, to achieve a holistic study of this theme it is paramount to understand the origin of the right to privacy and how it has evolved up to date in light of the ever changing technological atmosphere where movement of data has become easier and cheaper. In addition, the research is geared

towards recommending practical legal reforms that take into account the pace of development in technology.

1.12 Limitations of the study

The project limited to the information accessible to the author and that there is a possibility of some invaluable pieces of information that might not be within the reach of the author. Secondly, a research of this nature that is likely to impact on people's lives requires time to interact with people and establish their nuances and financial resources which are beyond the scope of this research. In addition, the literature available to the author focuses on other jurisdictions with scarce information, if any, about Kenya and as such the author is likely to borrow the principles applicable to other jurisdictions and recommend them to remedy lapses in Kenya without taking into account the difference in social, cultural, economic, moral and religious factors.

1.13 Chapters break down

Chapter one is the introduction of the project. It gives the background of the research question and objective. In addition, it provides the theoretical framework upon which the research is based and provides views of various scholars in the literature review. In addition, it elaborates the methodology, ethical considerations and limitations of the study.

Chapter two traces the history of right to privacy and its development in online social networking sites with focus on international and regional platforms.

Chapter three identifies inadequacies in the legal regime of right to privacy in Kenya and addresses the attempts by Kenya to have specific legislation on protection of the right to privacy

which also cover online platforms including social networking sites. It further compares the laws on privacy and data protection in other foreign South Africa, Ghana and Europe.

Chapter four analyses the legal regime on right to privacy in Kenya. It gives the brief background of development of online and social networking sites in Kenya and its growth.

Chapter five highlights conclusions from the first 4 chapters and makes a case for engendering the best practices and reform for inadequacies in the legal regime thereby suggesting raft of reforms.

CHAPTER 2

HISTORY OF THE RIGHT TO PRIVACY AND ITS DEVELOPMENT: RELEVANCE IN THE LEGAL FRAMEWORK OF KENYA

2.0. Introduction

This chapter examines the historical background of privacy and its development. It further illustrates the applicability of the right to privacy in social networking sites while at the same time highlighting the key factors which have facilitated the need for protection of right to privacy. It further defines the scope and meaning of right to privacy while at the same time assessing the impact of both technology and internet in the development of privacy particularly online.

The chapter also analyses the principles of international law relevant in the protection of privacy while highlighting the challenges of traditional principles of sovereignty and horizontal applications of rights in enforcement of right to privacy and how the same have been dealt with by the United Nations and other regional organizations.

2.1 The Origin of Privacy and its protection

Scholars argue that privacy existed from time immemorial but not in the form it is currently manifested.[128] They argue that ancient societies including various religions had some concepts of privacy premised on the Bible and Qu'ran,[129] for instance, Adam and Eve upon realizing that they were naked attempted to cover themselves with twigs.[130] Noah got drunk and uncovered himself. His son Ham upon seeing his nakedness informed his brothers who moved swiftly without looking at him and covered him. When he woke up and learnt about what had happened he cursed Ham. Thus a demonstration of how violation of privacy attracted dire consequences.[131]

History of privacy is more of patchwork thus prompting various pundits to urge different positions. Some historians trace it back from 1361 when penalties were imposed on peeping toms based on their invasion to privacy.[132]A good example was William Pitt, Earl of Chatham who once elevated privacy of homes as one of protected rights by declaring that a cottage of the poorest man is a revered place that even the King of England could not enter without his permission.[133] This was later followed by the British Lord Camden who defended privacy of homes and papers by quashing warrants for such intrusion in 1765 declaring that enjoyment of life is premised on protection of papers.[134] The Freedom of Press Act and Access to Public Records Act of 1776 was

128 Adrienn Lukács, 'What is Privacy? The History and Definition of Privacy,' (2016) University of Szeged, Paris 1 available at http://publicatio.bibl.u-szeged.hu/10794/7/3188699.pdf accessed on 03/07/2019

129 Ibid (n50)

130 Genesis 3

131 Genesis 9: 22-24

132 1361, England

133 Speech, March 1763, in Lord Brougham Historical Sketches of Statesmen in the Time of George III First Series (1845) vol. 1 cited in www.oxfordreference.com accessed on 11/09/2019

134 Vashek Matyáš, Simone Fischer-Hübner, Daniel Cvrcek, Petr Švenda The Future of Identity in the Information Society: 4th IFIP WG, 2008 Springer Brno Czech Republic

specifically enacted in Sweden to protect private information.[135]France, for instance prohibited unauthorized disclosure of private information from as early as 1858.[136]

On the other hand the documented history indicates that colonial America (1492 -1763) had protection of privacy and considered a home to be a person's castle.[137] This right extended to sanctity of the body which was first considered in 1881 Michigan Court that punished a non-medic bachelor who intruded upon a woman during child birth and the Court awarded damages.[138] This decision was applied in other cases which fell for determination on protection of right to privacy.[139]

This right then extended to correspondence including mails and telegraphic communications[140] and later on private and personal documents in possession of an individual were included.[141] Judge Cooley classified attempted physical touch as a tort and used the term right to be left

135 Freedom of Information and Access to Government Records Around the World135 David Banisar135 Privacy International July 2002 accessed on http://www1.worldbank.org/publicsector/learningprogram/Judicial/AccessInfoLaw%20Survey.rtf accessed on 03/07/2019.

136 Elisabeth Logeais and Jean-Baptiste Schroeder, The French Right of Image: An Amiguous Concept Protecting the Human Persona, 18 Loy. L.A. Ent. L. Rev. 511 (1998). Available at: https://digitalcommons.lmu.edu/elr/vol18/iss3/5 accessed on 07/10/2019

137 Ibid (n53)

138 Supra n54. The Court held that: It would be shocking to our sense of right, justice and propriety to doubt even but that for such an act the law would afford an ample remedy. To the plaintiff the occasion was a most sacred one and no one had a right to intrude unless invited or because of some real and pressing necessity.

139 Union Pacific Railway Co. v. Botsford 141 U.S. 250 (1891). in which the Court held that: The inviolability of the person is as much invaded by a compulsory stripping and exposure as by a blow. To compel any one, and especially a woman, to lay bare the body, or to submit it to the touch of a stranger, without lawful authority, is an indignity, an assault, and a trespass.

140 Supra (n50)

141 Boyd v. United States, 116 U.S. 616 (1886). The Court held that: It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offence; but it is the invasion of his indefeasible right to personal security, personal liberty and private property. . . . [A]ny forcible and compulsory extortion of a man's own testimony or of his private papers to be used as evidence to convict him of crime or to forfeit his goods, is within the condemnation of that judgment. In this regard the Fourth and Fifth Amendment run almost into each other.

alone.[142] This was later adapted to describe various aspects of protection of privacy which existed in common law at that time.[143]

In 1890, an article was published reacting to publication of events of a party of Mr. Warren's daughter in a highly personal and embarrassing way by journalist in what became known as 'yellow Journalism.'[144] However, this did not bring to light the right to privacy until Courts in New York[145] began issuing orders against those found to have acted in ways considered as infringement of rights bordering on privacy. However, the same did not last long as a Court in Michigan rejected it[146] albeit on conditions which even subsequent authors agreed amounted to reasonable limitations such as where a person was dead or a public figure.[147]

The key rejection of right to privacy was witnessed by Courts in New York which denounced the idea of distinct right to privacy.[148]It reasoned that the acts of intrusion into people's private lives occasioned no injury and that it had a potential of prompting numerous claims. But this ignited public outcry which led to enactment of legislation in New York which criminalized and made a tort the invasion on right to privacy.[149]

142 Ibid n2

143 Ibid n3

144 Ibid

145 Mackenzie v. Soden Mineral Springs Co., 27 Abb. N. Cas. 402, 18 N.Y.S. 240 (Sup. Ct.1891) (use of name of physician in advertising patent medicine enjoined); Marks v. Jaffa,6 Misc. 290, 26 N.Y.S. 908 (Super. Ct. N.Y. City1893) (entering actor in embarrassing popularity contest) ; Schuyler v. Curtis, 147 N.Y. 434, 42 N.E. 22 (1895) (erection of statue as memorial to deceased; relief denied only because he was dead).

146 Atkinson v. John E. Doherty & Co., 121 Mich. 372, 80 N.W. 285 (1899).

147 Supra (n3)

148 Roberson v. Rochester Folding Box Co. 171 N.Y. 538, 64 N.E. 442 (1902).

149 Supra (n34)

Subsequently, courts adopted the views of Samuel Brandeis and confirmed existence of a distinct right to privacy. [150] Later on, the Courts were divided as to whether or not the right to privacy existed and Courts in America were quick to accept the position in consonance with the common law principles.[151] The variation in views of different pundits has led to failure to define right to privacy thus presenting a situation where it can merely be described.[152]

Based on the above analysis it is clear that Louis Warren and Samuel Brandeis were not the founders of right to privacy but they played a big role in magnifying its presence at a time when most people did not take it seriously and the opinion of Courts were varied. Notably, the history paints an oblique picture of the roles of legislature and executive in development of privacy protection. On the other hand the judiciary is projected as the epicentre of protection of privacy.

2.2 Developments in Right to Privacy

During the formative stage privacy was viewed from the perspective of oppressive governments that violated the rights of individuals and groups which led to the international organizations formulating instruments focused on the protection of people's fundamental rights.[153] However, such instruments were formulated with the foresight on the strengths of individuals and corporations to the extent that the right to privacy is enforceable against individuals and legal persons in what has been called horizontal application.[154] This application has been described

150 Supra n58. The Court held that: One who desires to live a life of partial seclusion has a right to choose the times, places, and manner in which and at which he will submit himself to the public gaze. Subject to the limitation above referred to, the body of a person cannot be put on exhibition at any time or at any place without his consent. . . It therefore follows from what has been said that a violation of the right of privacy is a direct invasion of a legal right of the individual.

151 Equality and Human Rights Commission, What is the European Convention on Rights, available on https://www.equalityhumanrights.com/en/what-european-convention-human-rights

152 Supra n86

153 Sedley (n8)

154 Ibid

realignment from historical attacks on the state powers to engendering positive conduct of individuals.[155]

The right to privacy in 17th to 19th Century guaranteed protection to homes, children, sex, medical, financial, family life, personal correspondences and private documents.[156] The same subsists to date albeit in a developed way.

It is notable that the focus was to prevent the intrusion by the government and its agents, little was thought about individuals being threats to privacy of other individuals notwithstanding horizontal application and progressive realignment of human rights envisaged in international Conventions and Protocols.[157]

But this shortcoming has been compounded by voluntary disclosure of confidential and private information. Thus human beings are not merely a threat to the privacy of others but to themselves too.[158]There are few instances of accidental or ignorant disclosure based on failure to understand operations of various technological devices and platforms which seem to have prompted the right to erasure of data if no longer needed otherwise known as and being forgotten.[159]

The advanced technological devices and platforms for instance the internet, micro cameras and mobile phone cameras have rapidly changed and even enhanced invasion of one's own privacy—or that of others.[160] For instance, consider information on blogs or social networking sites where people post their photos in both merry and sad moments which end up being shared by their

155 Equality and Human Rights Commission, What is the European Convention on Rights, available on https://www.equalityhumanrights.com/en/what-european-convention-human-rights

156 Ibid n82

157 Ibid

158 Harvard Law Review Association, 'The Right to Privacy' (1898) Harvard Law Review 12, 207.

159 Thomson Judith, 'The Right to Privacy' (1975) 4 Philosophy and Public Affairs 295.

160 Supra n68

mutual friends and other people within seconds.[161] The same could expose private information about such people thereby ending up breaching their very right of privacy and making it difficult for regulators to intervene.[162]

The law on right to privacy has developed to cover emerging technological advances including telephone interception, wiretapping, bugging, computers and other modes of communication and data collection and storage called for development of law on right to privacy.[163] However, there is a perception that these advancements develop faster that the pace at which laws are reviewed hence difficulty in realization of full enjoyment right to privacy.

These devices, in as much as they have improved and enhanced interaction between human beings they remain the greatest threats to privacy as argued above.[164] This has made the web so enticing to the extent that it is difficult for people to refrain from sharing data online which they would otherwise not share offline.[165]

Various search engines including but not limited to Google[166] can store vast information about net users which is likely to be handed over to third parties for various considerations. Yahoo paid USD 117 Million in settlement of class action on data violations on allegations email addresses, phone numbers, dates of birth, other account information, as well as security passwords of billions

161 Ibid

162 Ibid. p.11:' Privacy has been commoditized. On the one hand individuals now have the possibility to profit from the manipulation of their privacy—whether by allowing it to be displayed in carefully organized and packaged slices, as celebrities of all kinds do; or by offering it up on the altar of the public gaze, as those wishing to be famous, or only to 'connect', as Big Brother demonstrates.

163 Ibid (n60)

164 Supra (n 68)

165 Ibid

166 Ibid (n56)

of users.[167] Thus, a legal regime focused on both preventive and curative measures comes in handy especially if it has mechanisms of enforcement.[168]

Ian Walden argues that in the modern world intangible information is an asset and that a substantial portion of such information is personal data which reveals a lot about individual's intimate lives to the world which breaches protection of privacy while at the same time avails itself as valuable commodity that has ready demand.[169]In 2018 the world was shocked when a whistle-blower disclosed how Cambridge Analytical[170] collected data from Facebook and used the same to build a psychological warfare tool allegedly used in the US elections of 2017.[171]

Indeed, the whistle-blower highlighted correspondences showing that top managers of Facebook Inc., were aware of the data breaches. This led to the Federal Trade Commission (FTC) imposing fine of USD 5 Billion on Facebook Inc.[172] Other Countries also fined and condemned Facebook based on the said breaches to wit UK's data protection watchdog imposed a fine of £500,000 noting that Facebook committed "serious breach" while Canada's data watchdog held that Facebook committed "serious contraventions" of its privacy laws.[173]

The aforesaid instances clearly demonstrated how personal information is invaluable and thus need for legal regime to protect the same while maintaining the delicate balance of the interests of the society as a whole against business or personal needs of an individual.[174] Today, protection of

167 https://topclassactions.com/lawsuit-settlements/privacy/data-breach/918019-yahoo-data-breach-class-action-settlement/ accessed on 10/10/2019

168 Ibid (n63)

169 Supra n92

170 US based Consultancy firm

171 https://www.bbc.com/news/world-us-canada-48972327 accessed on 19/08/2019

172 Ibid

173 Supra (n132)

174 Ibid (n65)

personal data has exceeded the previous parameters of laws relating to intellectual property, trespass and interception of communication amongst other regimes.[175]

English Courts established misuse of private information as tort proof of which lied on the claimant proving that he reasonably expected privacy in relation to aspects of his life or data threatened by unauthorised disclosure.[176] The available remedies included injunction which would be considered upon assessing the proportionality of competing public interests seeking the disclosure.[177]

2.3.1 Privacy and data protection

Europe has evolved different perspective on privacy by focusing of data protection which is embedded in the legislative framework. Hence focus is mainly on controlling the automated processing data of personal or intimate nature.[178] On the other hand, America notwithstanding the fact that it is a hub of major technology companies, does not have a unified code or regulations on privacy or data protection with most laws relevant to privacy being highly fragmented inconsistent, and gap ridden thus leading scholars to describe its legal regime on privacy as unwieldy and conflicting.[179]

Scholars embracing the European perspective suggest that data protection be confined to the protection of information under the control of the state on security, safety, sovereignty, morality

175 Supra (n 53).

176 Supra (n67).

177 Supra (n58).

178 Supra (n 53).

179 Solove, Daniel J. and Schwartz, Paul M., ALI Data Privacy: Overview and Black Letter Text (September 20, 2019). Available at SSRN: https://ssrn.com/abstract=3457563 or http://dx.doi.org/10.2139/ssrn.3457563 accessed on 20/09/2019

and cultural interests.[180] That argument is not farfetched because other countries such as Italy, Denmark and Austria extended data protection to companies and other entities thereby prohibiting intrusion into their activities and information.[181] In contract the law on data and related rights only protect the public but not the private organizations or entities.[182]

In the United Kingdom the Courts have distinguished between privacy and data to the extent that the former is engaged *ex post*, once the abuse arises, while the latter is *ex ante* obligations imposed on those processing data.[183] Other distinctions have also been made in terms of enforcement thus whereas an individual presents before a court an issue of breach of privacy, data protection is advanced by regulatory authority in establishing compliance on the part of an agency charged with processing personal data.[184] There are thus instances of confluence between data and privacy while in other instances of divergence in personal and substantive scope.[185]

2.3.2 The General Data Protection Regulations (GDPR)

The European Union guaranteed protection of privacy and data under Data Protection Directive[186] until 27th April, 2016 when the General Data Protection Regulation otherwise known as GDPR was adopted and later enforced from 25th May, 2018.[187] However, each member state has an

180 Ibid (n70)

181 Ibid

182 David Rolph, 'Politics, Privacy and the Public Interest: A Case Study from Australia' <http://ssrn.com/abstract=2070443> accessed 22/09/2019.

183 Supra (n67)

184 Ibid (n72)

185 Ibid

186 DPD 95/46/EC available on https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

187 General Data Protection Regulation (EU) 2016/679

option to modify GDPR for instance United Kingdom was previously under the regime of Data Protection Act of 1998 which has now been repealed by Data Protection Act of 2018.[188]

GDPR notes that protection of data is one of the fundamental rights. It demands that that data processors view their work to serve mankind and nothing else.[189] However, the Right is not absolute and must be balanced against other rights with the guidance of the principle of proportionality.[190]

It is also notable that GDPR protects personal data which it considers broadly as information that can be used as identifier of data subject either directly or indirectly including physical, physiological, mental, economic, cultural or social identity[191] and may include information such as credit card number, accessing address, codes, password, bank statements, criminal record among others. [192]

GDPR enshrines such principles regarding processing of personal data,[193] lawfulness of processing,[194] conditions for consent,[195] conditions applicable to child's consent in relation to information society services,[196] processing of special categories of personal data,[197] processing

188 http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

189 GDPR Clause 4

190 GDPR recitals 1 and 4

191 GDPR Art 2

192 https://ec.europa.eu/eip/ageing/standards/ict-and-communication/data/directive-9546ec_en

193 GDPR Art 5

194 Ibid Art 6

195 Ibid Art 7

196 Ibid Art 8

197 Ibid Art 9

of personal data relating to criminal convictions and offences[198] and processing which does not require identification.[199]

It grants rights to data subjects which include transparency and modalities which covers transparent information, communication and modalities for the exercise of the rights of the data subject,[200] information and access to personal data which relates to information to be provided where personal data are collected[201] or not[202] and right of access;[203] rectification and erasure[204] and right to be forgotten;[205] right to restriction of processing;[206] notification obligation alterations or restriction of processing;[207] right to data portability;[208] right to object and automated individual decision-making which covers right to object;[209] and restrictions and objections. [210]

On the other hand Data Protection Act of the United Kingdom provides for six principles including requirement lawful and fair data processing;[211] specified, explicit and legitimate processing;[212] adequate, relevant and not excessive personal data to be collected;[213] accurate and

198 Ibid Art 10

199 Ibid Art 11

200 Ibid Art 12

201 Ibid Art 13

202 Ibid Art 14

203 Ibid Art 15

204 Ibid Art 16

205 Ibid Art 17

206 Ibid Art 18

207 Ibid Art 19

208 Ibid Art 20

209 Ibid Art 21

210 Ibid Art 22

211 Data Protection Act, 2018 Section 35(1)

212 Ibid s36(1)

updated personal data;[214] storage only if necessary[215]and secure processing.[216] Besides, it guarantees rights of subject data at such awareness,[217] access,[218]alteration including erasure, correction and being forgotten[219] and power over automation.[220] Further, one is entitled to enforce his/her rights in an established institution.[221]

It is evident that Data Protection Act is a clear reflection of the principles contained in the GDPR including imposition of safeguards on data sharing with other countries.[222]

Based on foregoing arguments, it is evident that there exist instances of overlaps and interlinks in both protection of data and privacy all over the world. However in Kenya the Constitutional foundation of privacy and related rights does not make the explicit distinction with both data protection being covered under principles of privacy.[223] The right to rectification of inaccurate data under the Kenyan Constitution is considered as an offshoot of data protection in other jurisdictions.[224] The interlink between these two aspects of rights is envisioned in the Data

213 Ibid s37(1)

214 Ibid s38(1)

215 Ibid s39(1)

216 Ibid s40(1)

217 Ibid s44

218 Ibid s45

219 Ibid s46 to 48

220 Ibid ss 49 and 50

221 Ibid

222 Chapter 5 DPA,2018

223 Ibid n12 Art.31

224 Ibid n12 Art 35(2) of the Constitution, 2010; see GDPR on correction of misleading personal data is considered under data protection within the European Union.

Protection Act[225] which considers privacy as the main area of protection while data is merely a subset therof.[226]

2.3.3 Right to be forgotten

The Data Protection Act, 2019 provides for correction or erasure of unnecessary, irrelevant and inaccurate data or those acquired unlawfully.[227] This obligation is imposed on data controllers, processors and their agents or third parties in possession of such data.[228] This provision reflects the right of data subject to be forgotten under erasure envisaged under the GDPR.[229]

Right to be forgotten is exercised where the data is unnecessary for the intended purpose, consent has been withdrawn and the processing or retention of data violates the Regulations.[230] This is also applicable to the internet just like in offline data processing indeed the data controllers and processers must advise their agents and third parties processing data on their online platforms to comply with the obligation to dete the impugned data.[231]However, there are exceptions to this right for instance in exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, on the grounds of public interest in the area of public health, for archiving

225 Act No. 24 of 2019 Laws of Kenya

226 Data Protection Act, 2019 which proposes to give effect to Article 31 of the Constitution which is right to privacy. Its object is regulate the collection, retrieval, processing, storage, use and disclosure of data of persons.

227 Ibid n.223 s 40 .

228 Ibid

229 Article 17

230 GDPR iArt 17

231 Ibid iClause i66

purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims.[232]

The Court of Justice of European Union considered the right to be forgotten in *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González*,[233]where Mr Costeja Gonzalez was involved in insolvency proceedings relating to social security debts in the late 1990s.[234] These proceedings were reported in a regional newspaper in Spain in 1998 and the article was later made available online.[235] Mr Costeja Gonzalez, who was named in the report, asked the newspaper to delete the piece arguing that the insolvency proceedings were concluded and it was no longer of relevance.[236]

The newspaper refused to erase the data on the basis that the Ministry of Labour and Social Affairs had ordered its publication.[237] Mr Costeja Gonzalez also asked Google Spain to remove links to the newspaper in its search results when his name was entered as a search term in the Google search engine.[238] Data Protection Authority in Spain upheld the complaint against Google requesting that the contested links be removed from Google's index of search results hence the reference.[239]

The Court decided that the fundamental rights to privacy and data protection should, 'as a rule' supersede both the commercial interest of the search engine operator as well as the interest of the general public.[240] It further held that the processing of data which is

232 Ibid iArticle i17(3)

233 Google iSpain iSL, iGoogle iInc. iv iAgencia iEspañola ide iProtección ide iDatos, iMario iCosteja iGonzález Case iC-131/12

234 Ibid

235 Ibid

236 Ibid

237 Ibid

238 Ibid

239 .Ibid

240 .ibid

inadequate, irrelevant or excessive might also be incompatible with the directive hence where the data is incompatible with the provisions of the directive relating to data quality, the information and links in the list of the results must be erased if unnecessary not only because of its prejudicial nature.[241]

2.3.4 Courts on obligations of data controllers and rights of data subject

The Court of Justice of European Union considered the obligations of websites in protection of data in the case of *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV*[242] a German consumer protection association, brought a lawsuit against Fashion ID on the ground that the use of that plugin resulted in a breach of data protection legislation on the ground that transmission to Facebook of visitors' personal data occurred without the data subjects' consent and in breach of the duties to inform set out in legislation to protect data of personal nature.[243] Fashion ID's website featured the Facebook 'Like' button, which allowed visitors of the website who are Facebook users to "like" articles and post them on Facebook's social network which meant that every time a visitor consulted the website, his or her personal data (namely, information concerning his or her IP address and browser string) was transmitted to Facebook, which also placed different kinds of cookies on the visitor's device.[244]

The Court held that Fashion ID was a controller of data jointly with Facebook, with respect to the activity consisting of collection of personal data and disclosure to Facebook.[245] It distinguished that Fashion ID was only liable for the first phase of collection and bound by the duty to make the data subjects aware of the processing and the obligations concerning the legal basis of the

241 .Ibid .

242 Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV Case C-40/17

243 Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV.243 Verbraucherzentrale NRW Case C-40/17

244 ibid

245 ibid

processing.[246] However it could not be held responsible for subsequent processing once the data was transferred to Facebook.[247]

Notably the Court applied provisions of Directive 95/46/EC which are similar to duties under the GDPR which places an obligation on joint controllers to the extent that website operator(s) and provider(s) of plugin(s) who act as joint controllers must enter into an arrangement accessible to data subject.[248]

Currently conflicting rights and obligations of data subjects and controller or processors was highlighted In *Społeczna Inicjatywa Narkopolityki (SIN) vs Facebook,*[249]where Civil Society Drug Policy Initiative a Polish NGO which has for many years conducted educational activities concerning the harmful consequences of drug use, was removed from Facebook and Instagram fan pages without any warning or clear explanation on the basis that their posts were characterized as 'in violation of *Community Standards*'.[250] It challenged this in District Court of Warsaw arguing that private censorship by Facebook was unlawful and contradicted its free speech or freedom of online expression. The Court granted interim measure restraining Facebook from blocking or removing SIN from its pages pending hearing of the case.[251]

246 ibid

247 ibid

248 Article 26 GDPR

249 https://edri.org/sin-vs-facebook-first-victory-against-privatised-censorship/

250 Ibid

251 Ibid

2.4 Internet and privacy

The assessment of protection of privacy in modern society is incomplete without mention of the internet. History points at usage of various devices in study of right to privacy but the introduction and use of internet as platform for communication has altered how right to privacy is viewed.[252]

Internet was a mere interconnection within the US Department before it evolved as a tool of research in various Universities.[253] Thereafter, in early 1980s the internet was commercialized in various countries and the number of users grew steadily.[254] African countries joined the internet in early 1990s.[255] Various social networking sites were founded from the year 2003-Myspace, 2004-Facebook on July, 2010 the 500millionth signed in.[256] Because of the surging number of internet users, new challenges were created ranging from technological ethical challenges to misuse of the platform.[257] In addition, anonymity continuously conflicted with accountability and trust. All these challenges prompted the idea of regulation.[258]

In Kenya, the internet is said to have arrived in mid 1990s with the attendant explanation that the then political environment stifled growth and free flow of information specifically in telecommunication sector. The state used its agencies to ensure the repression including issuance

252 Barry M. Leiner, Vinton G. Cerf, David D. Clark,Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, Stephen Wolff, A Brief History of the Internet, Internet Society, Volume 39 Issue 5, October 2009 New York, USA.

253 Raphael Cohen-Almagor, Internet History, International Journal of Technoethics, 2(2), 45-64, April-June 2011 45 University of Hull, UK

254 Ibid

255 Muriuki Mureithi, The internet Journey for Kenya: The Interplay of Disruptive Innovation and Entrepreneurship in Fueling growth in B. Ndemo, T.Weiss, (Eds), Digital Kenya: An enterpreneural revolution in the making (2017) Palgrave Studies of Entrepreneurship in Africa.(Palgrave Macmillan)

256 There are 4.1 billion Internet users in the world as at December 2018. Available at https://hostingfacts.com/internet-facts-stats/

257 K. Jaishankar (Ed) Book Review of Hate Crimes in Cyberspace, Centre for Cyber Victim Counselling (CCVC), International Journal of Cyber Criminology, Vol 8 Issue 2 July Editor-in-Chief: - December 2014, India, Hate Crimes in Cyberspace. (2014). Danielle Keats Citron, Harvard University Press, Cambridge, Massachusetts.

258 Ibid note 49

of declarations against internet.[259] But around the year 2000 the government changed its perspective and viewed internet as a tool of development. This was the moment when the political activists believed that democratization was taking shape in Kenya thus resulting in change of regimes in 2002 accompanied with enjoyment of various rights which were hitherto prohibited.

The growth of internet in Kenya reached 112 per cent by 2017, translating to an estimated 51.1 million Internet users in a country of about 45 million…showing that people mostly access internet by multiple devises for instance through mobile devices, home internet, work spaces and cyber cafes among other avenues.[260]

2.5 Privacy and technology

Technology arguably is a double edged sword as it equips a person to safeguard his privacy while at the same time exposes such a person to others' scrutiny. However, authors are divided about protection of privacy in the technology driven world with some indicating that it is a mirage[261] while others are optimistic that such rights exists and ought to be protected.[262]

The anti-privacy protection supporters/theorists argue that a user of online medium can always be tracked both at the time of use and thereafter. Digital footprints they argue are traced by capturing the Internet Protocol (IP) address and as such he is making informed choice of plunging into the dangerous territory knowing consequences very well.[263]Besides, the use of cookies, E-mail or

259 Abdul Noorani, 'The Right to Privacy' (2005) 40 Economic and Political Weekly 802; the then agency was Kenya Posts and Telecommunications Corporation

260 Business Daily, How Many Internet Users are in Kenya; 10/01/2018 Available at https://www.businessdailyafrica.com/corporate/tech/How-many-Internet-users-are-in-Kenya/4258474-4259072-htn83lz/index.html accessed on 03/09/2019

261 Ibid (n74)

262 Supra (n 49).

263 personally identifiable information that is automatically captured by another computer when any communications link is made over the internet. Whenever a person browses, visits a site, sends an email or chats online, he leaves his distinct IP address behind which can be searched either through IP registration databases or by conducting a trace route, to determine an approximate physical location of an IP address.

document bugs, globally unique identifier, spyware, web bugs, and online digital profiling have made it possible for the user's privacy to be exposed to third parties who willingly choose to utilize them while knowing the inherent danger.[264]Their views reflect the thinking around the principle of *volenti non fit injuria.*

But the pro-privacy protection group admits the existence of these threats and risks but view the same as incentives for regulation and protection thus calling for action against the misusers and abusers.[265] Their argument suggests and rightly so that it is difficult to ignore technology in the modern world.[266]

2.6 Right to Privacy and International Law

Internationally every individual is accorded right to privacy as is evident the United Nations Universal Declaration of Human Rights[267] has been described by scholars as the *"Magna Carta of Contemporary International Human Rights law*."[268] It grants each and every person the right to privacy without any form of distinction. It prohibits subjecting people to arbitrary interference with privacy of families, homes or correspondence, nor to attacks upon their honour and reputation.[269]

264 Privacy International, '"The Right to Privacy in the Digital Age"'.

265 Supra (n 37).

266 Ibid (n37)

267 Article 12; https://www.un.org/en/universal-declaration-human-rights/ accessed on 06/08/2019

268 Richard B. Lillich, The Human Rights of Aliens in Contemporary International Law, 41 (Manchester University Press 1984); Universal Declaration of Human Rights, G.A. Res. 217A(III), U.N. GAOR, 3d. Sess., Supp. No. 13, at 71,U.N. Doc. Al810 (1948).

269 Universal Declaration of Human Rights Article 12

The privacy envisaged under this article is broad and includes physical, personal and informational. Besides, the ICCPR[270] also guarantees right to privacy in similar terms as UDHR. The same principles are envisaged in the OECD principles on right to privacy[271] they include non-discrimination meaning that sensitive data such as racial or ethnic origin should not be compiled at all;[272] power to make exceptions to wit limitations only for reasons of national security, public order, public health or morality;[273] and supervision and sanctions demanding that the data protection authority shall offer guarantees of impartiality, independence vis a vis persons or agencies responsible for processing and technical competence.[274]

The Guidelines were modified by the Council in 2013 and crystalized to 8 principles of data quality, individual participation, collection limitation, purpose specification, security safeguards, use limitation, openness and accountability.[275] Indeed, their applicability is beyond the borders of member states as the Guidelines envisage international application especially the states likely to interact with OECD member states.[276]

The United Nations General Assembly in 2013 adopted resolution and established The Right to Privacy in the Digital Age.[277] It was worried about unauthorized surveillance exhibited by various

270 No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

271 OECD Working Party of Information Computers and Communications Policy (ICCP) created in 1977 made its regulations in 1980.

272 Ibi

273 Ibid

274 Ibid (n 143).

275 OECD Guidelines Governing The Protection of Privacy and Transborder Flows Of Personal Data, Articles 7-15

276 Ibid

277 Resolution 68/167adopted by the General Assembly on 18 December 2013 [on the report of the Third Committee (A/68/456/Add.2)] available at https://undocs.org/pdf?symbol=en/a/res/68/167 accessed on 26/11/2019

member states and considered the same vilation of fundamental right expressed.[278] The Assembly affirmed that the need for equality in rights online as offline to guarantee rights of online users.[279] It demanded state protection and respect of digital communication including review of procedures, practices and enactment of laws to prohibit surreptitious intrrception or surveillance of correspondence both offline and online and regulating control or processing of personal data as envisaged under international law.[280]

Later, the High Commissioner for Human Rights presented a report to the Assembly on the protection of privacy and related rights in the digital age which noted the significance of the internet, smartphones and Wi-Fi enabled devices to development in human interaction. [281] The Commission also pointed out the high cases of violation of privacy and demanded higher levels of protection by member states calling for prohibition of unauthorized, unjustified, arbitrary and unlawful intrusion into privacy of families, communication offline or otherwise, homes of individuals by ensuring legislative guarantees and oversight mechanism.[282]

The General Assembly adopted the report on the right to privacy in the digital age[283] thereby calling upon all states to respect and protect privacy and related rights.[284] The General Assembly encouraged the Human Rights Council to consider the possibility of establishing a special procedure to further the aim of protecting privacy and related rights.[285]

278 Ibid

279 Ibid

280 Ibid

281 UN General Assembly, The right to privacy in the digital age, Report of the Office of the United Nations High Commissioner for Human Rights, 2014, A/HRC/27/37

282 Ibid

283 Resolution 69/166 adopted by the General Assembly on 18 December 2014 [on the report of the Third Committee (A/69/488/Add.2 and Corr.1)] available at https://undocs.org/en/A/RES/69/166

284 Ibid

285 Ibid

The Human Rights Council in 2015 by a resolution appointed a Special Rapporteur on the right to privacyfor a period of three years.[286] The resolution directed the Special Rapporteur, amongst other responsibilities, to report on alleged violations of the right to privacy including in connection with the challenges arising from new technologies.[287]

The foregoing international instruments make sense only if the protection of privacy is understood in terms of the modern interactions of various people globally. This is because technology has created global village to the extent that transactions and correspondent between individuals in different corners of the world are able to transact and communicate in real time.[288] Consequently, large amounts of data of personal nature cross national boarders either through internet or manual transfer of media (hard-disk and note book computers) and personal digital assistants.[289] This has been enhanced by the development of the internet into a market like platform which has facilitated emergence of speedy means of communication.[290] This clearly highlights the need to have laws and regulations geared towards protecting personal data taking into account the challenges of data havens, development of technology and voluntary breaches.

The issue of sovereignty which is central to the international principle has been identified as one of the key issue in privacy law because of data collection, retention and sharing.[291] This is because of the ideas of flow of data and processing of the same within and outside the traditional jurisdictions of states.[292] Besides, cyberspace is linked to physical installation and devices which must be

286 adopted resolution 28/16 at its 28th session available on https://www.un.org/unispal/wp-content/uploads/2018/03/A.72.53.pdf

287 Ibid

288 Ibid n9

289 Camrin L. Crisci, 'All the world is not a stage: Finding a right to privacy in existing and proposed legislation (2002) 2 N.Y.U Journal of Legislation and Public Policy, 215

290 Supra n52

291 Patrik Hummel, Matthias Braun, Steffen Augsberg,and Peter Dabrock Friedrich-Alexander, Sovereignty and Data Sharing, ITU Journal: ICT Discoveries, Special Issue No. 2, 23 Nov. 2018 International Telecommunication Union, 2018 available at https://www.itu.int/en/journal/002/Pages/default.aspx

292 Ibid

located in a given territory at any material time.[293] This has led to consideration of cyberspace in terms of both cyber sovereignty and strategic autonomy the former signifying control of data whether it originates from or passes over the traditional territory state the latter suggesting control over technology infrastructure, data processing and storage.[294]

In 2004 the United Nations established the United Nations Governmental Group of Experts (UNGGE) to interrogate the issue of sovereignty in cyber space among other related issues and the group recommended that state sovereignty was applicable in cyberspace.[295] The decision meant that the Law of Armed Conflict was applicable in cyberspace, as well as all rights and obligations tied to principles of sovereignty. [296]

2.7 Conclusion

This Chapter has analysed the historical background of privacy and intertwined the same with modern technological developments. It has also assessed the place of privacy and its relationship with data protection thus concluding that in Kenya these terms are synonymous while in other jurisdiction they have different scopes. This chapter has also established that both the internet and technology have greatly influenced privacy and for full realization of the same Kenya must adjust its legal regime on protecton of privacy to tackle modern challenges. To achieve this, the Chapter highlights the protection of privacy guaranteed by various international instruments and best practices which Kenya ought to adopt to revamp its legal regime on right to privacy.

293 Annual report of the United Nations High Commissioner for Human Rights and reports of the Office of the High Commissioner and the Secretary-General on the right to privacy in the digital age, 2014 available on https://www.ohchr.org › Issues › DigitalAge › A-HRC-27-37_en

294 Ibid

295 Digital Watch Observatory, 2017

296 The Tallinn Manual on the International Law Applicable to Cyber Warfare and the Tallinn Manual 2.0

CHAPTER 3

THE INADEQUACIES IN THE LEGAL REGIME ON RIGHT TO PRIVACY IN KENYA

3.0 Introduction

This chapter identifies some of these inadequacies in protecting privacy and the failed attempts which Kenya has made towards legislating on protection of privacy. It explains that these attempts are clear pointer of the challenges, risks and threats which calls for urgent enactment of modern and harmonized legislation.

It also explains the need to learn from both South Africa and European Union which have progressive laws for protection of privacy and related rights in the modern technologically developed world and online.

3.1 Constitutional privacy

In the previous chapters we saw how the Constitution, 2010 guarantees protection of privacy in broader sense from physical space, against intrusion into solitude, unauthorized searches and seizures, information on private life or affairs which borders on trust and confidentiality. The Constitution also guarantees freedom of expressions which allows communication but prohibits instances which might violate reputation. On the other hand freedom of the media and access to information allows for instances when information can be sought and produced notwithstanding

that it limits other rights including privacy.[297] Besides, the Constitution provides for limitation of rights and freedoms thus listing right to privacy as amongst the limitable rights.[298]

The Courts have further grappled with enforcement of privacy and related rights in the ever changing technological world and observed that there is need for regulation of the online interaction due to emerging threats which could further inhibit realization of full enjoyments of privacy as envisaged in the Constitution.

The government has made various attempts to address the inadequacies in the law on privacy by proposing various bills which unfortunately have fallen short of Constitutional guarantees thus leading to either being blocked by the Courts or the legislative arm failing to enact the same. Indeed, some of the existing laws have been used by the state actors to infringe upon the right to privacy, mainly in the security department.

3.2 Security Laws

The security laws in Kenya have been perceived to be superior laws which seem to trample all other laws for instance the National Intelligence Service Act[299] expressly limits right to privacy especially for sspects of offences specified in the Act[300] by intercepting, monitoring, tapping or investigating their correspondence either online or offline.[301] The state agents are allowed to obtain any information, material, record, document or thing and for purposes of investigation by

297 Constititution of Kenya Art. Articles 34 and 35

298 Ibid Art 24 and 25

299 National Intelligence Service (NIS) Act (2012)

300 Ibid s 35 and 42

301 Ibid

searching, recovering and availing data or property without the normal due process as envisaged in other sections of the Act which might be abused in certain circumstances.[302]

3.3 The Prevention of Terrorism Act (2012)

This is another legislation which limits privacy as it allows interception, curtailment, investigation, surveillance or interference with communication of suspects of terrorist offences.[303] Indeed, no measures are put in place to regulate the limitation envisaged under Article 24 of the Constitution.[304] Consequently, whereas this is well meaning legislation, it is open to abuse which could violate right to privacy.

3.4 The Security Laws (Amendment) Act (2014)

Prevention of Terrorism Act explicitly limits enjoyment of privacy envisaged under the Constitution by allowing survailance of communication for purposes of detection, investigation, deterring and disrupting terrorism.[305] The framework of such limitation is left to the Minister through regulations.[306] Thus, this Act creates a new regime contrary Article 24 of the Constitution by leaving limitation to fundamental right to the Minister to be achieved through regulations and not by legislation.[307]

Thus the security laws are major impediments to realization of protection of privacy as they allow the state actors to violate this right without adhering to the Constitutional thresholds.[308] Hence the

302 Section 36 and 45 of the Act

303 Prevention of Terrorism Act, Section 35

304 Ibid n12

305 The Security Laws (Amendment) Act (2014) s 69

306 Ibid

307 Privacy International, 'The Right to Privacy in the Digital Age'(2018)

308 Ibid

need to reform these laws to have limitations of privacy and related rights defined as envisaged under the Constitution.

3.5 Attempts to enact legislation on Right to Privacy

Kenya has made various attempts to enact a legislation envisaged under the Constitution to provide for full enjoyment of right to privacy and appurtenant limitations. However, numerous attempts have either failed or have been found to contravene other freedoms envisaged in the Constitution as elaborated below.

3.5.1 Computer Misuse and Cybercrimes Act 2018

Kenya enacted Computer Misuse and Cybercrimes Act on 16th May, 2018 and came into operation on 30th May, 2018.[309] Pundits while contesting its provisions believed that this legislation was way overdue considering that Kenyans were relying on outdated statutes contained in the 1948 Penal Code[310] and the 1998 Kenya Information and Communication Act to try digital crimes.[311]

The objects of the Act as contained in the Memorandum of Objects and Reasons indicated that:

> The Bill proposes to provide a framework to prevent and control the threat of cybercrime, that is, offences against computer systems and offences committed by means of computer systems. Kenya Vision 2030 recognizes ICT as one of the key

309 Computer iMisuse iand iCybercrimes iAct i2018

310 Chapter i63 iof iLaws iof iKenya

311 Mercy iMutemi, iTaming iThe iInternet: iThe igood, ithe ibad iand ithe iugly iparts iof ithe iComputer iMisuse iand iCybercrimes iAct i2018. iAccessed ion i09/06/2019 ihttps://www.theelephant.info/features/2018/05/24/taming-the-internet-the-good-the-bad-and-the-ugly-parts-of-the-computer-misuse-and-cybercrimes-act-2018/ iaccessed ion i12/10/2019

drivers of socioeconomic development in the Republic and an enabler in achieving the middle income country status. [312]

The objects of this Act includes protection of the confidentiality, integrity and availability of computer systems, programs and data; preventing the unlawful use of computer systems; facilitating the prevention, detection, investigation, prosecution and punishment of cybercrimes; protecting the rights to privacy, freedom of expression and access to information as guaranteed under the Constitution; and facilitating international co-operation on matters covered under the Act.[313]

The Act targeted unauthorized access, interference, interception, disclosure of password or access code, access with intent to commit or facilitate further offence, illegal devices.[314] It also enhanced penalties for offences involving protected computer system, cyber espionage, false publications, child pornography, computer forgery, computer fraud, cyber stalking and cyber bullying, aiding or abetting in the commission of an offence, offences by a corporate and limitation of liability, recovery of assets, and offences committed through the use of a computer system just to demonstrate its punitive nature.[315]

The word privacy is merely mentioned in the Act as an obligation of state agents during investigations to the extent that they are under duty to take measures to prepare and ensure that the real-time collection or recording of content data is carried out while maintaining the privacy of other users, customers and third parties and without the disclosure of

312 i http://kenyalaw.org/kl/fileadmin/pdfdownloads/bills/2017/ComputerandCybercrimesBill_2017.pdf iaccessed ion i12/10/2019

313 Computer Misuse and Cybercrimes Act

314 Ibid

315 Ibid ss 4 to 21

information and data of any party not part of the investigation.[316] Thus, the Act failed to address the inadequacies bedeviling realization of full enjoyment of right to privacy envisaged under the Constitution.

The Act is still in force but some of its provisions were suspended by the Court pending hearing and determination of the Petition, they included sections 5, 16, 17, 22, 23, 24, 27, 28, 29, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 48, 49, 50, 51, 52 & 53.[317]

3.5.2 The Cyber security and Protection Bill, 2016[318]

This Bill was proposed by the Senate of Kenya, its principal objects as per its Memorandum of Objects and Reasons include to provide for the enhancement of security in cyberspace extending to prohibition, prevention, detection, response, investigation and prosecution of cybercrimes and to establish institutional mechanism to address issues of cyber security in Kenya.[319]

The reasons for the Bill included recognition that the world is increasingly run through the use of computer technology and through this virtual system, people are able to send money, store large amount of data, communicate across continents at the touch of a button, control security infrastructure, run businesses and enhance human connectivity. However while computers have increased human connectivity and have a direct impact on development, they also pose a risk to the users.[320]

316 Sections 52 and 53 of the Act

317 Bloggers Association Of Kenya (Bake) V Attorney General & 5 Others [2018] eKLR

318 http://kenyalaw.org/kl/fileadmin/pdfdownloads/bills/2016/CyberSecurityandProtectionBill_2016.pdf accessed on 12/10/2019

319 The Cyber security and Protection Bill, 2016 available on http://kenyalaw.org/kl/fileadmin/pdfdownloads/bills/2016/CyberSecurityandProtectionBill_2016.pdf accessed on 12/10/2019

320 Ibid

The Kenyan government has been rolling out various services on digital and electronic platform which are threatened by potential cyber insecurity which might disrupt the delivery of essential services and in effect cause irreparable harm to the economy and lives of people.[321] Thus, computers and virtual connectivity have also exposed society to certain vulnerabilities which the Bill sought to address and prohibit with a view to protect privacy, life and property.[322]

3.5.3 The Data Protection Bills of 2018

Kenya has made various attempts before enact legislation before Data Protection Act, 2019 instance in 2018 it had two Bills one by the Ministry of Information, Communications and Technology while the other by the Senate both with slightly different objects *to wit* the Memorandum of objects of the Senate Bill which states that the principal object of the Bill is to protect personal data collected, used or stored by both private and public entities.[323]

The Bill recognized that data protection forms part and parcel of the expectation of the right to privacy.[324] This Bill provided for the legal framework for protection of a person's privacy in instances where personal information is collected, stored, used or processed by another person.[325] In Kenya the right to privacy is protected under Article 31 of the Constitution. Therefore, this Bill sought to operationalize Article 31 of the Constitution, in particular Article 31(d) and (c).[326]

The Bill by the Ministry suggested that principal object of the Bill was to govern the enforcement of Article 31 of the Constitution of Kenya on the Right to Privacy and particularly sub-article

321 Ibid

322 Ibid

323 Memorandum of Objects of the Senate Bill

324 Ibid

325 Ibid

326 Ibid

31 (c) and (d), by setting out the requirements for the protection of Personal Data processed by both Public and Private Entities as a facet to the right to privacy.[327] The Bill also sought to outline the key principle that shall govern the processing of personal data by both public and private entities, while outlining the rights of data subjects and the duties/ responsibilities of data controllers and processors.[328] The Bill also provided for its jurisdictional scope and applicability scope of the right to personal data protection. In terms of Kenyan data subjects and personal data processed in Kenya and outside Kenya and with limitations to the right.[329]

The Ministry's Bill listed 17 principles and obligations including principles of personal data protection, rights of a data subject, exercise of rights by data subject, collection of personal data, duty to notify, lawful processing of personal data, conditions for consent, processing of personal data relating to a child restriction on processing, automated individual decision making, objecting to processing, processing for direct marketing, right to data portability, limitation to retention of personal data, right of rectification and erasure, security safeguards to personal data and notification and communication of breach.[330]

On the other hand the Senate Bill suggested 20 objects and principles which included principles of data protection, right to protection of privacy, limitation, collection of personal data, quality of information, rights of the data subject, duty to notify, when agency may not notify, exemptions, prohibition of profiling, data processing, protection and security of personal data, notification of security compromises, access to data, correction of information, retention of

327 Memorandum of Objects of ithe National Assembly Bill

328 Ibid

329 Ibid

330 Clauses 22 ito 38 of the Bill

information, misuse of information, commercial use of data, use of unique identifiers and interference with personal data.[331]

The Ministry's Bill suggested protection of personal sensitive data but only classifying health but leaving other data to be classified as such by Data Commissioner.[332] On the other hand the Senate Bill listed special data under part three.[333] Such data is classified to include religious or philosophical beliefs, race or ethnic origin, trade union activities, health, personal data of children, political persuasion and trans-border flow of information.[334] The foregoing evidently showed that the Senate Bill was more detailed than that of the Ministry.

On enforcement, the Ministry proposed that the data processors and controllers be registered,[335] formation of the Office of the Data Protection Commissioner[336] and elaborate procedures on dealing with trans-border flow of information.[337] On the other hand the Senate Bill proposed oversight and enforcement mechanism with powers to investigate and settle complaints.[338]The Bill suggesting enforcement of right to privacy highlighting the need to protect privacy and personal data thereby listing limitations while [339] the Ministry's Bill focusing on enforcement of data protection.

331 Clause 4 to 23 of the Senate Bill
332 Ibid n301
333 Clause 24 to 3a of the Senate Bill
334 Ibid
335 Clause 15-21 of the Bill
336 Ibid Clause 5 to 14
337 Ibid Clause 44-46
338 Clauses 32-36 of the Senate Bill
339 Ibid Clause 4

3.5.4 The Data Protection Bill, 2019

The 2019 Bill was thus framed upon merging some of the ideas in both Senate and the Ministry's proposals. However, the 2019 Bill reflected so much of the Ministry proposals while ignoring the Senate proposals albeit the Bill would have been robust if both 2018 Bills were harmonized.

The Memorandum of Objects and Reasons of the 2019 Bill proposed that the principal object of the Bill is to govern the enforcement of Article 31 of the Constitution of Kenya on the Right to Privacy and particularly sub-article 31 (c) and (d), by setting out the requirements for the protection of personal data processed by both Public and Private Entities as a facet to the right to privacy. It also seeks to outline the key principle that shall govern the processing of personal data by both public and private entities, while outlining the rights of data Subjects and the duties/ responsibilities of data controllers and data processors and finally, provides for its jurisdictional scope and applicability scope of the right to Personal Data protection. In terms of Kenyan data subjects and personal data processed in Kenya and outside Kenya and with limitations to the right.[340]

3.5.5 Data Protection Policy, 2018

The Draft Data Protection Policy recognizes the Constitutional and international foundations of the right to privacy in Kenya and undertakes to outline legal framework of enforcing the right to privacy.[341] Besides, its states that its development is prompted by growth in data collection and processing based on rapid development of technology and increasing access to the internet in Kenya.[342]

340 http://www.parliament.go.ke/sites/default/files/2017-05/Data_Protection_Bill_2018.pdf accessed on 02/09/2019

341 Privacy and Data Protection Policy 2018- Kenya available at http://www.ict.go.ke/wp-content/uploads/2018/08/Kenya-Data-Protection-Policy-2018-15-8-2018.pdf accessed on 12/10/2019

342 Ibid

It also takes note of the international practices and jurisprudence which have recognized right to privacy as human right, thereby, making the protection of Personal Data a key pillar in enforcement of other rights and freedoms enshrined in the Constitution. It states that in order to harness the benefits of the digital economy and mitigate the harms consequent to it, formulating a Data Protection policy is critical for Kenya.[343]

Its aim is to protect personal data in order to guard against misuse and to eliminate the unwarranted invasion of privacy. Besides, its purpose is to lay foundation to enforce Article 31 of the Constitution of Kenya, by developing privacy and data protection laws and to inform on the management of Personal Data in the information life cycle and the commitment of the Kenya Government to protect the Personal Data including the Personal Sensitive Data.[344]

3.5.6 The Kenya Information and Communication (Amendment) Bill 2019

The Bill seeks to regulate social media platforms by licensing of social media platforms, controlling sharing of information by a licensed person, creating obligations to social media users, registration of bloggers and seeking to give responsibility to the Communications Authority to develop code conduct for bloggers.[345]

3.5.7 The Data Protection Act, 2019

On 08/11/2019 the Data Protection Act No. 24 of 2019 was enacted along the Ministry's proposals with commencement date of 25/11/2019. The principal object of the Act is to give effect to the

343 Ibid

344 Supra (n223)

345The Kenya Information and Communication (Amendment) Bill, 2019 available http://www.parliament.go.ke/sites/default/files/2019-10/Kenya%20Information%20and%20Communication%20%28Amendment%29%20Bill%2C%202019-No.2_compressed.pdf accessed on 12/10/2019.

right to privacy as provided for in Article 31(c) and (d) of the Constitution by setting out the requirements for the protection of personal data processed by both public and private entities.[346] Further, the Act outlines the key principles that shall govern the processing of personal data by both public and private entities, while setting out the rights of data subjects and the duties of data controllers and data processors.[347]

It establishes the Office of the Data Commissioner, provides for the appointment, qualifications, functions, powers, removal of the Data Commissioner[348] and the registration of both data controllers and data processors hence outlining the application procedure including necessary thresholds and exemptions, duration of the licence, cancellation of the registration, periodic audits by the Data Commissioner and possibilities for the designation of the data protection officer.[349]

It also lists the principles and obligations of data controller(s) and processors together with rights of data subject which include the processing of personal data, the rights of data subjects and exercise of such rights, conditions for consent, principle of data portability, retention and rectification of personal data, data protection assessments, processing of data belonging to children and notification procedures in instances of breaches.[350]

It covers the grounds for processing of sensitive personal data including further categorization of sensitive personal data[351] and conditions for the transfer of personal data outside Kenya including provision of safeguards prior to transfer of personal data out of Kenya.[352]

346 The iData iProtection iAct iNo. i24 iof i2019 isections i3 i& i4

347 Ibid

348 Ibid iSs.5-17

349 Ibid Ss.18-24

350 Ibid Ss. 26-43

351 Ibid Ss. 44-47

352 Ibid Ss. 48-50

Exemptions to processing of personal data are captured in the Act together with development of a data sharing code.[353]

It also caters for the enforcement mechanism of how the Office of the Data Commissioner may exercise the powers conferred on it.[354] Finally, it provides for offences including the unlawful disclosure of personal data, general penalties, the development of codes and guidelines and the consequential amendments.[355]

The structure of the Act and its contents evidently reflect the ideals contained in the GDPR and the African Union Convention on Cyber Security and Personal Data Protection.[356]For instance, Article 11 and 12 demands for establishment of an authority to oversee the implementation of laws on privacy and data protection laws and regulations. Indeed, the principles on sensitive personal data which even though the Act identifies only health and grants the Data Commissioner discretion to classify, the Convention also provides for protection of such data.[357]

The Convention provides for the obligations relating to conditions governing personal data processing which include basic principles governing the processing of personal data which include principle of consent and legitimacy, principle of lawfulness and fairness, principle of purpose, relevance and storage, accuracy, transparency and principle of confidentiality and security.[358]Rights of data subjects are also explained including right to information[359], right of

353 Ibid,Ss. 51-55

354 Ibid, Ss. 56-66

355 Ibid, Ss. 72-75

356 https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

357 Article 14 of the Convention

358 African_union_convention_on_cyber_security_and_personal_data_protection Art 13

359 Ibid Article 16

access,[360] right to object[361] and right of rectification or erasure.[362] Obligations of data controllers include confidentiality,[363] security,[364] storage[365] and sustainability.[366]

The foregoing are closely related to principles in the GDPR such as principles relating ito processing of ipersonal data,[367] lawfulness of iprocessing,[368] conditions for consent,[369] conditions applicable to child's consent in relation to information society services,[370] processing of special categories of personal data,[371] processing of personal data relating to criminal convictions and offences,[372] processing which does not require identification.[373]

The Data protection Act, 2019 is therefore well founded and its effectiveness or efficiency in realizing the right to privacy under Article 31 will only be determined by its enforcement upon the establishment of the Office of the Data Commissioner. However, it is also notable that it could have been more robust if the proposals by the Senate in their Bill were included.

3.6 Lessons from other Jurisdictions

This paper draws some of the lessons on enforcement of right to privacy from Ghana, South Africa, and European Union. The former has similar Constitutional provision to that of Kenya while the latter reflects modern growth and development in enforcement of right to privacy.

360 Ibid Article 17
361 Ibid Article 18
362 Ibid Article 19
363 Ibid Article 20
364 Ibid Article 21
365 Ibid Article 22
366 Ibid Article 23
367 IIbid Art 5
368 Ibid Art 6
369 Ibid Art 7
370 Ibid Art 8
371 Ibid Art 9
372 Ibid Art10
373 Ibid Art 11

Besides, the Constitution of Kenya, 2010 allows application of international instruments and best practices and European Union has manifested up to date development in both realization of both right to privacy and data protection.

3.6.1 Ghana

In 1970s the Courts of Ghana grappled with the issue of protection of privacy with the same being ventilated in the case of *University of Cape Coast v Anthony*[374] albeit the Appeal failed on the aspect of invasion of privacy. The Court considered that it is a right worth protecting and also noted limitation of its enforcement such as consent which absolutely waives its existence.[375]

Later in 1992 protection of privacy was enshrined in the Constitution which guaranteed that:

> No person shall be subjected to interference with the privacy of his home, property, correspondence or communication except in accordance with law and as may be necessary in a free and democratic society for public safety or the economic well-being of the country, for the protection of health or morals, for the prevention of disorder or crime or for the protection of the rights or freedoms of others.[376]

It has been observed that Ghanaians cherish group lifestyles and that individualized kind of privacy might be untenable thus intrusions by clan or family members into private sphere is not deemed as a serious violation like that of third parties such as the media.[377]

The Constitutional foundation of privacy in Ghana is distinct from that of Kenya, both in the 1969 and 2010 Constitutions. This is because the former imposed express limitations while the latter

374 University of Cape Coast v Anthony [1977] 2 GLR 2

375 Ibid

376 Constitution of the Republic of Ghana 1992,article18(1)&(2

377 Supra n50

did not. Such express limitations have been lauded as proper balancing mechanism and clear delineation of the boundaries of privacy hence certainty in enforcement.[378] In addition Ghana has limited spheres of privacy protected in the Constitutions which include protection of home, property or communication[379] compared to Kenya which protects person, possessions, family and personal information.[380] Remedies for violation of right to privacy in Ghana flow from common laws of England and decisions of superior Courts of Ghana which include injunctions and damages.[381]

Ghana has enacted the Electronic Transactions Act[382] being substantive law with its attendant and procedural aspect and Mutual Legal Assistance Act,[383] with specific provisions on international cooperation on cybercrime and electronic evidence.[384] Besides, it has the Economic and Organized Crime Act,[385] Security and Intelligence Agencies Act,[386] Data Protection Act[387] and Anti-Money Laundering Act.[388]

The Data Protection Act of Ghana Provides for principles of data processing which include privacy of the individual, minimality, consent, justification and objection, collection of personal data; data for specific purpose; Data subject to be made aware of purpose of collection; Retention of records; Further processing to be compatible with purpose of collection; Quality of information; Registration of data controller; Security measures; Data

378 Ibid

379 Constitution of Ghana, Article 18

380 Ibid n12, Art 31

381 Ibid n215

382 Electronic Transactions Act, 2008 (ETA)

383 Mutual iLegal iAssistance iAct, i2010 i(MLAA)

384 https://www.thehaguesecuritydelta.com/media/com_hsd/report/135/document/Cyber-security-trends-report-Africa-en.pdf

385 Economic and Organized Crime Act, 2010 ("EOCA")

386 Intelligence Agencies Act, 1996 ("SIAA")

387 Data Protection Act ("DPA"), 2012

388 Anti-Money Laundering Act, 2008 AMLA

processed by data processor or an authorized person; Data processor to comply with security measures; Notification of security compromises; Access to personal information; Correction of personal data and manner of access.[389]

It also accords the data subject rights which include access to personal information, to amend personal information, prevent processing of your personal information, freedom from automated decision making, prevent processing of personal data for direct marketing purpose, seek compensation through the courts and to complain to the Data Protection Commission.[390]

3.6.2 South Africa

The Constitution of the Republic of South Africa[391] guarantees protection from search of person, home and property; seizure of possessions and prohibition of infringement of privacy of communication.[392]

It is evident that informational privacy under article 31(c) of the Constitution of Kenya is wider than Section 14(d) of the South African Constitution. However, South Africa has made robust procedure for security apparatus to intercept communications through judicial authorization as captured in relevant regulations.[393] RICA does not allow for user notifications save that the reports are compiled and presented before Parliament's Joint Standing Committee on Intelligence. This differs from the decision of the Court of Appeal of Kenya which held that the

389 Data Protection Act Sections 17-34 available at https://nita.gov.gh/wp-content/uploads/2017/12/Data-Protection-Act-2012-Act-843.pdf

390 Ibid, Section 35

391 The Constitution of the Republic of South https://www.acts.co.za/constitution-of-the-republic-of-south-africa-act-1996/index.html accessed on 02/09/2019

392 Ibid, Section 14

393 Regulation of Interception of Communications and Provision of Communications Related Information Act (RICA) (2002).

investigative agencies can only seek search warrants if a suspect does not comply with notice to produce documents, data or evidence.[394]

It has also enacted legislation to protect personal data *to wit* the Protection of Personal Information Actwhich regulates the processing of personal information by public and private bodies in a manner that gives effect to the right to privacy. [395] It also provides for limitations aimed guaranteeing other related rights and important interests.[396]

It has been lauded as progressive as it has internalized international principles which include[397] requirement that the processing of information is limited which means that personal information must be obtained in a lawfully and fair manner and can only be used for the specified purpose it was originally obtained for. [398]

Besides, it limits the further processing of personal information if the processing takes place for purposes beyond the original scope that was agreed to by the data subject, the processing is prohibited.[399] It also demands that the person who processes the information must ensure the quality of the information by taking reasonable steps to ensure that the information is complete, not misleading, up to date and accurate.[400]

The processor must have a degree of openness, ensure that the proper security safeguards and ensure that measures to safeguard against loss, damage, destruction and unauthorized or unlawful access or processing of the information, has been put in place; he must be

394 Director of Public Prosecutions v Tom Ojienda t/a Prof Tom Ojienda & Associates Advocates & 3 others [2019] eKLR

395 http://www.justice.gov.za/inforeg/docs/InfoRegSA-POPIA-act2013-004.pdf

396 Chapter 3 of POPI

397 https://www.michalsons.com/blog/data-privacy-in-south-africa/150

398 Ibid

399 Ibid

400 Ibid

accountable to ensure that the measures that give effect to these principles are complied with when processing personal information.[401] Finally, the data subject must be able to participate by accessing the personal information that a responsible party has on them and must be able to correct the information.[402]

Besides, various online abuses and misuses are covered under the Electronic Communications and Transactions Act[403] which prohibits various aspects of cybercrimes including the interference with data in a way that causes the data to be modified, intentional and unauthorized access or interception of any data, destroyed or rendered ineffective and the unlawful production, sale, distribution or use of a device that is designed primarily to overcome security measures for the protection of data.[404]

In *Bernstein and Others v Bester NO and Others*[405] the Court considers right to privacy as a fundamental right which is only subject to other competing rights of members of the society. It observes that intimate and personal data ought to be accorded higher level of protection than data which is readily available in the public domain. This view is consistent with the position of Justice Ackermann in *National Coalition for Gay and Lesbian Equality and Another v Minister of Justice and Others*[406] that privacy creates private sphere which guarantees autonomy to individuals to nature relationship thus attempts to erode the same impinge of that aspect of self-determination.[407]

401 Ibid

402 ibid

403Electronic Communications and Transactions Act 25 of 2002(ECTA) and http://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/Activities/SA/docs/SA-1_Legislation/South%20Africa/ElecComm.PDF accessed on 05/10/2019

404 Ibid

405 CCT 23/95 [1996] ZACC 2

406 CCT 11/98) [1998] ZACC 15

407 Ibid

The courts in South Africa have held that instances of actionable intrusion include bugging a person's room, listening to private telephone conversations, spying on someone while she was undressing, reading private documents, unauthorized blood tests and harassment.[408]

3.7 Conclusion

The inadequacies in the legal regime on right to privacy in Kenya are evident in this Chapter. Whereas Kenya has a very broad Constitutional underpinning of the right to privacy under Article 31, the specific legislation to enable full realization took time to be achieved but yet to be tested.[409] It is notable that Kenya has various statutes on different aspects of right to privacy either protecting or limiting the same. This Chapter argues that these pieces of legislation have failed to address the modern threats to privacy especially online.

The attempts by legislature in Kenya to enact a comprehensive legislation to guarantee right to privacy is a clear indication of the desire to have data protection law prompted by modern challenges posed by fast developing technology. All the Bills highlighted in this Chapter notes the issues of technological developments and modern threats and risks online.

The Chapter has discussed protection of privacy in South Africa and Ghana which have had data protection laws and enforcement as model guides on enforcement to right to privacy. The former has nearly similar constitutional provision to that of Kenya while the latter has been constitution for long. Besides, the principles of data protection after codifying its privacy laws envisaged in both GDPR and the African Union Convention on Cyber Security and Personal Data Protection are evident in the Data Protection Act, 2019 thus in terms of legal instrument Kenya has now

408 Jonathan Burchell, The Legal Protection of Privacy in South Africa: A Transplantable Hybrid, vol. 13.1 Electronic Journal Of Comparative Law, (March 2009), available at http://www.ejcl.org.

409 Data Protection Act, 2019

manifested the desire to protect privacy. However, elimination of inadequacy identified in this Chapter will only be assessed when the enforcement commences that it when all the proposed institutions are established and the provisions of the Act is enforced.

CHAPTER 4

THE LEGAL REGIME ON THE RIGHT TO PRIVACY IN KENYA:

4.0 Introduction

This chapter is a study on the legal regime on right to privacy in Kenya. It provides the background of Constitutional foundation of the right to privacy since independence to 2010 while at the same time ventilating reasons for the slow development in the protection of privacy rights in Kenya. It also interrogates some of the pieces of legislation which have been considered as protecting the right to privacy in Kenya.

Besides, it highlights jurisprudence so far developed by the Kenyan Judiciary on right to privacy which is also applicable to social networking sites. It identifies the legal challenges, including lack of specific legislation on privacy, that Kenyan Courts and other institutions continue to face in light of the fast growing number of users in social networking sites and proceeds to analyze how the same impact on right to privacy.

4.1 Constitutional privacy

In Kenya, privacy was founded on the Repealed Constitution which provided that:

> *"Protection for the privacy of his home and other property and from deprivation of property without compensation."*[410]

It focused more on protection of intrusion of homes and other property. Basically, it did not guarantee privacy of physical space, person or information.[411] The High Court observed that

410 Ibid n11 s 70(c)

Section 70(c) of the Repealed Constitution protected specific infringement of privacy of person, home and property/possessions.[412]

The foregoing view was expanded upon promulgation of Constitution of Kenya 2010.[413] This has offered a broad and liberal view on protection of privacy by guaranteeing privacy of person, home, property, possessions.[414] It further protects information relating to family or private affairs from being revealed or required unnecessarily[415] and prohibits infringement of communication.[416]

It is notable from the two provisions that the Kenyan Constitution guarantees wider right to privacy than the South African version. It is notable that the repealed constitution of Kenya had a very limited scope of privacy. Besides, there is an obligation on all state and non-state actors to respect all fundamental rights and freedoms.[417]

Besides, the scope of the constitutional right to privacy in Kenya is also wider than duty of confidentiality under the common law. Therefore, by protecting privacy in communications, the Constitution, 2010 guarantees right to privacy in online networking sites where majority of citizens interact. This broad clause could be explained by various technological developments including ease of access to various electronic devices and the internet. Further, this is broadened by the applicability of international laws and principles including best practices envisaged under the Constitution.[418]

---

411 Ibid n11 s 70

412 J W I & Another v Standard Group Limited & Another [2015] eKLR

413 Constitution of Kenya, 2010, Art 31.

414 Ibid 31(a) & (b)

415 Ibid 31(c)

416 Ibid 31(d)

417 Ibid Art 20 & 21

418 Supra n413 Art 2(5) & (6)

The Constitution of Kenya provides for freedom of expression which guarantees every person the right to freedom of expression, which includes freedom to seek, receive or impart information or ideas.[419] This freedom is the foundation of social media as people seek, receive or impart ideas online. The limitations to this freedom both online and offline include the rules against propaganda for war, incitement to violence, hate speech, or advocacy of hatred that constitutes ethnic incitement, vilification of others or incitement to cause harm; or is based on any ground of discrimination.[420] Besides, the Constitution is explicit that in the exercise of the right to freedom of expression, every person shall respect the rights and reputation of others.[421]

4.2 Internet in Kenya and right to privacy

The right to privacy as envisaged in the Constitution of Kenya, 2010 would better be understood in light of the study of internet as a medium of communication within which people correspond and that both protection and violation of those rights remain prominent issues worth considering.

Internet as a platform of communication was introduced in Kenya in 1993 and later in 1995 the first internet service provider was licensed.[422] Besides, mobile phones became widely available around 2000 after the Communications Commission of Kenya now Communications Authority of Kenya licenced Safaricom and Kencell in 1999.[423]

419 Ibid, Art 33(1)

420 Ibid, Art 33(2).

421 Ibid, Art33(3)

422 Francisca Mweu, "Overview of the Internet in Kenya," International Telecommunication Union (prepared for African Internet & Telecom Summit, Banjul, The Gambia, June 5–9, 2000)

423 Freedom on the Net, 2011 https://www.refworld.org/pdfid/4dad51b7f.pdf

Between 2000 and 2009 various pieces of infrastructure were put in place which have made internet accessible to many people in Kenya. These factors include installation of undersea cables (Seacom and The East African Marine System (TEAMS) which has led to reduction of the cost of internet, availability of phones capable of connecting to the internet and absence of government interference.[424] Indeed, research shows that Kenyans are the most intensive mobile internet users in Africa, with each user browsing an average of 525 pages per month.[425]

Online users in Kenya by March, 2019 were at 43,329,434 people compared to 200,000 people in 2000 hence the internet growth of 21,564%. [426] This growth is further explainable by the fact that between 1993 when the internet was introduced in Kenya to 2019 the environment for enjoyment of various rights has been expansive.[427] Indeed, about 20 years ago the state declared internet illegal through an advertisement by the then Kenya Posts and Telecommunications Corporation thus limiting its usage.

Further that the devices for accessing internet such as computers and phones were scarce.[428] The growth therefore is attributable to ease of access and promulgation of 2010 Constitution which apart from providing for broad right to privacy has also guaranteed environment for enjoyment of the same through other rights and freedoms.[429] The challenge with this populous access of the internet is the existence of abuse and misuse. Unfortunately, the internet in Kenya lacks specific legislation or regulations to regulate its usage and protect innocent users from abuse and misuse.

424 CCK, "Quarterly Sector Statistics Report, Second Quarter Oct-Dec 2009/2010."

425 Victor Juma, "Mobile Internet on Course to Becoming Top Earner for Firms," Business Daily, April 22, 2010, available at http://allafrica.com/stories/201004210995.html.

426 www.internetworldstats.com accessed on 08/10/2019

427 Ibid (n153)

428 Ibid

429 Ibid n413 Art 26 to 39

4.3 Other legislation on Right to Privacy

Kenya has various pieces of legislation which protect privacy, confidentiality and data. However, they have been perceived as sector specific and focused on offline privacy and data and not modern online privacy challenges. Some of these include the Official Secrets Act;[430] Children's Act;[431] HIV and AIDS Prevention and Control Act;[432] Witness Protection Act;[433] Banking Act,[434] Credit Reference Bureau Regulations 2013,[435] Central Bank Draft Credit Reference Bureau Regulations, 2019;[436] and Capital Markets Act;[437] the Penal Code,[438] Access to Information Act;[439] Kenya Information and Communications Act (KICA);[440] Private Security Regulation Act;[441] Public Archives and Documentation Service Act[442] and the Elections (Technology) Regulations, 2017[443]. All of these statutes fail to comprehensively deal with potential risks/threats to privacy and data protection due to advanced modes and means of data processing.[444]

The Penal Code[445] prohibits the intrusion of the modesty of any person by stripping them.[446] The seriousness of this offence is evident in the penalty of imprisonment of 10 years for conviction. It

430 Chapter 187 of Laws of Kenya

431 Chapter 141 Laws of Kenya

432 Act No. 14 of 2006

433 Act No. 16 of 2006

434 Chapter 488 Laws of Kenya

435Legal Notice No. 5 available at https://www.centralbank.go.ke/wp-content/uploads/2016/08/CREDIT_REFERENCE_BUREAU_REGULATIONS_2013.pdf

436https://www.centralbank.go.ke/wp-content/uploads/2019/05/DRAFT-CREDIT-REFERENCE-BUREAU-REGULATIONS-2019.pdf

437 Chapter 485A Laws of Kenya

438 Chapter 63 of Laws of Kenya

439 Act No. 31 of 2016 Laws of Kenya

440 Chapter 411 A Laws of Kenya (Revised in 2015)

441 Act No. 13 of 2016

442 Chapter 19 Laws of Kenya

443Legal Notice No. 67, April, 2017 Kenya Government Printers available at https://www.iebc.or.ke/uploads/resources/8lJsH5aTCd.pdf

445 Chapter 63 of Laws of Kenya

is a pertinent aspect of protection of right to privacy save that it is based on physical acts of stripping whereas the online 'stripping remains undefined.[447] In addition, the Penal Code had criminal defamation which restricted publications, print, writing, painting, effigy or other means by which the defamatory matter is conveyed to be so dealt with, either by exhibition, reading, recitation, description and delivery or otherwise.[448] The defamatory statements meant matter likely to injure the reputation of any person by exposing him to hatred, contempt or ridicule, or likely to damage any person in his profession or trade by an injury to his reputation.[449] The provision protected reputation both in life and death.[450]

In 2017 the High Court of Kenya declared criminal defamation as unconstitutional on the basis that it is a claw back to freedom of expression to the extent that it has a stifling and chilling effect on the right to speak and the right to know.[451] In addition, it noted that the gravity of the punishment imposed for this crime is clearly excessive and blatantly disproportionate. [452]

The Kenya Information and Communications Act[453] defines access, data and electronic record which points to the states view towards protection of online communication for instance, telecommunication system is defined as a system for the conveyance, through the agency of electric, magnetic, electro-magnetic, electro-chemical or electro-mechanical energy, of speech, music and other sounds, visual images, data, signals serving for the importation (whether as between persons and persons, things and things or persons and things) of any material

446 Ibid Section 251A. A person who intentionally insults the modesty of any other person by forcibly stripping such person, commits an offence and is liable, upon conviction, to imprisonment for a term not less than ten years.

447 Ibid

448 Penal Code, s. 194, 195 and 196.

449 Ibid

450 Ibid

451 Jacqueline Okuta & Another v Attorney General & 2 Others [2017] eKLR

452 Ibid

453 Chapter 411 A Laws of Kenya (Revised in 2015)

otherwise than in the form of sound, visual images or data, or signals aiding in the activation or control of equipment or gadget.[454] Electronic record is defined as record created in digital form by an information system, which can be conveyed within an information system or from one to another and stored in an information system or other medium.[455] These definitions clearly capture all forms of communications through online and offline channels of communications.

The Act prohibits interception of communications by services providers and disclosure of such information. Such illegal acts are punishable by fine of three hundred Thousand or imprisonment of 3 years.[456] Section 83 of the Act further prohibits unauthorized access of computers and mining data therefrom. In addition, section 93 of the Act prohibits the Commission and any other person from using information acquired during their normal business but which touch on personal or intimate matters of any individual or any business.[457] However, they are allowed to use such information upon obtaining the authorization or consent of the victim. The protection in the Act is drawn from the spirit of the Constitution and to capture other players the regulations under the Act extends the protection to licensees.[458]

4.4 The Kenyan jurisprudence on Right to Privacy

The Courts in Kenya have made positive steps towards protection of privacy as evident in decided cases. They have proffered purposive and broad interpretation of the Constitution and international instruments. This is reflected in various decisions both pre and post 2010

454 Ibid, S.2

455 Ibid

456 Ibid Section 31

457 Ibid n419

458 Kenya Information and Communications (Consumer Protection) Regulations (2010), s.15 (1).

"Subject to the provisions of the Act or any other written law, a licensee shall not monitor, disclose or allow any person to monitor or disclose, the content of any information of any subscriber transmitted through the licensed systems by listening, tapping, storage, or other kinds of interception or surveillance of communications and related data."

Constitution. In pre 2010 Constitution the Courts held that section 70 of the Constitution of Kenya, 1969 protected the right to privacy and that searches or access by public authorities to houses, ship, aircraft, vehicle, box or confiscation of things received from such places could only be achieved by search warrants issued by a judicial officer upon evidence on oath of the inevitability for such warrants.[459]

Thus, state agents are obligated to apply for search warrants to lawfully enter upon and search any premises, or to carry away any property from any person suspected of committing an offence.[460]Besides, the seized materials or possessions must be placed before Court to determine mode of disposal. The Court went further in holding that unauthorized searches by state actors is violation of right to privacy and that limitation thereto must be balanced against the purposes sought to be achieved.

The foregoing protection of right to privacy has been robust in post 2010 Constitution as manifested in various Court decisions. In *J W I & Another v Standard Group Limited & Another*[461]the Court observed that Section 70(c) of the Repealed Constitution protected right to privacy in a limited way focusing on physical space against arbitrary searches and seizure while the Constitution, 2010 has enshrined a broader and liberal protection of privacy in terms of what its scope as compared to protection offered under Section 70(c) of the Repealed Constitution.[462]

Since the Court was determining issues which preceded the Constitution, 2010 it heavily relied on and applied right to privacy under common law which includes access into a private residence, the reading of personal documents, evesdroping on to intimate conversations and the shadowing of a

459 Vitu Limited –vs- The Chief Magistrate Nairobi & Two Others, H.C. Misc. Criminal Application No. 475 of 2004

460 Standard Newspapers Limited & another v Attorney General & 4 Others [2013] eKLR

461 J W I & Another v Standard Group Limited & Another[2015] eKLR

462 Ibid

person.[463] Besides, it considered disclosure of personal information which have been accessed by a wrongful act of meddling and the disclosure of private facts in breach of a association of confidentiality together with dissemination of a person's photograph as part of an advertisement without the consent of the person.[464]

The Court held that a person remains the 'boss sovereign' over his personal space or solitude in which he has a 'right to be let alone' while guaranteeing that he would not injure other people.[465] Thus, non-consensual publication of the images of an individual violate protection of privacy because it derogates the privileged territory and autonomy of an individual by limiting the exclusive authority of determining conditions of his solitude or otherwise.[466] Similar to the finding by the Court in *Director of Public Prosecutions v Tom Ojienda t/a Prof Tom Ojienda & Associates Advocates & 3 others*[467] *that* the right to privacy entitles an individual to have control over his or her personal information and that the same should be shielded from unwarranted intrusion but the same cannot be claimed by third parties on behalf of the aggrieved individual.[468]

In *David Lawrence Kigera Gichuki v Aga Khan University Hospital*[469] the Court viewed protection of the privacy of a person to include prohibition to unlawful searches or seizures, or from unlawful dissemination of private information including the right to have such information as public records, photographs, communications, diaries and health records kept private and beyond the reach of third parties.[470] It elaborated based on decisions from the United States that it

463 Ibid

464 Ibid

465 Ibid

466 Ibid.

467Director of Public Prosecutions v Tom Ojienda t/a Prof Tom Ojienda & Associates Advocates & 3 others [2019] eKLR

468 Ibid

469 David Lawrence Kigera Gichuki v Aga Khan University Hospital [2014] eKLR

470 Ibid

has numerous riders for protection of public interests, health and security. In certain instances, the same can be limited by Court orders and provisions of laws regarding other rights.[471]

In *Kenya Legal and Ethical Network on HIV & AIDS (KELIN) & 3 others v Cabinet Secretary Ministry of Health & 4 others*[472] the High Court relied on South African jurisprudence with approval that a person's intimate sphere of life and the preservation of its basic preconditions must be granted utmost safeguard under privacy.[473] This is because there is a ultimate untouchable sphere of human freedom that is beyond intrusion from any public authority as it forms the basis of privacy.[474] However, this core is narrowly interpreted the moment an individual associates with persons outside such closest intimate sphere as his actions are deemed to attain a social dimension subject to various restrictions based on balancing of opposing interests and rights. [475]

Private affairs are those matters which occasion psychological and physical injury if disclosed because they are confidential by their nature and could expose the individual to humiliation, inhumane treatment and even limit his right to life.[476] In crafting limitations, the Court developed threshold borrowing from South Africa[477] beyond which the red flag of breach is raised which include the accessing data without consent of the Applicant, if the data in issue relate to personal life, where the data is used for unintended purpose and instances where the extent of publication is beyond limits of expectation of the Applicant.[478]

471 Barbra Georgina Khaemba v Cabinet Secretary, National Treasury & Another [2016] eKLR

472 Ibid

473 Bernstein v. Bester NO, 1996 (2) SA 75.

474 Ibid n449

475 Ibid.

476 Ibid n208

477 Mistry v Interim National Medical and Dental Council of South Africa (1998) (4) SA 1127 (CC).

478 Ibid

In the case of a constitutional breach of privacy the High Court has held that[479] the following issues must be taken into account to wit has the invasive law or conduct infringed the privacy envisaged in the Constitution and if so, is such an impingement justifiable in terms of the requirements laid down in the restriction's clause of the Constitution.[480] The Court believed that normative idea founding this broad consensus is that fundamental rights are owed to persons as a matter of human dignity and should be honored by all public and private persons or entities.[481]

The rights and freedom from degrading and inhumane treatment, privacy, due process and equal protection under the law are among the minimal rights that each person must enjoy to give meaning to life.[482] Drawing from David Feldman, the Court emphasized that certain kinds of treatments wich degrade humanity and dignity of human beings are inconsistent with rights and fundamental feedoms as they deprive humans of the basis of their lives.[483]

In *Roshanara Ebrahim v Ashleys Kenya Limited & 3 others* the Court held that publication of a person's private photographs by unauthorized person without the owner's consent is a violation of the person's right to privacy.[484] But such protection must serve a lawful purpose, the preservation of the applicant's dignity in conduct that accord with the law. This right cannot be invoked to protect private photographs the taking of which constitutes a criminal offence or which capture

479 M W K v another v Attorney General & 3 Other, High Court Petition No. 347 of 2015

480 Ibid

481 Ibid

482 Palko v. Connecticut, 302 U.S. 319, 325 (1937)

483 David Feldman, Human Dignity as a Legal Value -Part I, 1999 Pub. L. 682, 690-91.

484 Roshanara Ebrahim v Ashleys Kenya Limited & 3 others High Court Petition No. 361 of 2016

illegal acts or which depict reasonably objectionable conduct.[485] This is because a person's privacy presumes that there is legitimate expectation of protecting private spheres.[486]

The Court went ahead to find that it was illegal for a third party to disclose intimate photos without consent of the victim even if it was for the exposure of criminal activities.[487] But it intimated that such improper access could be utilized by the state agencies notwithstanding an outright warning that such agencies must respect the right to privacy in discharging their duties.[488]

On the other hand the negative obligation of the state agents from intrusion was evident in *M W K v another v Attorney General & 3 Others* where the Court found that Police conducting strip search in full glare of third parties was tantamount to violation of privacy. **[489]** It found that searching of any person that involves the exposure of that person's naked body, and in particular the most private parts thereof, to the gaze of another person, is degrading to the person being so exposed.[490] The Court summed up the common law and constitutional privacy as the main ground of its finding to wit the right to privacy as a self-determining personality right which magnifies a valuable aspect of one's personality.[491] The right is however not absolute as there are opposing factors such as maintaining law and order that can bear a substantial limitation on the right.[492] This manifests that careful balancing act of the protection of privacy and other factors is necessary.

In its decision in *Kenya Human Rights Commission v Communications Authority of Kenya & 4 Others*considered as Court's perspective on online privacy underscoring importance of the right to

485 Ibid

486 Ibid

487 Ibid

488 Ibid

489 M W K v another v Attorney General & 3 Other, High Court Petition No. 347 of 2015

490 Ibid

491 Ibid

492 Ibid

privacy, how new threats are emerging and preparation to tackle the same.[493] The Court accepted the constitutional and common law rights to privacy and moved ahead to interrogate emerging challenges on the basis that the autonomy of the individual must be viewed in light of his association with the rest of the society.[494] It considered the constitutional right to privacy of an individual within an environment where information technology governs virtually every aspect of life thus the issue of balancing the needs/opportunities and dangers posed to liberty in a digital world arise.[495]

The Court suggested that this balancing act can only be achieved if the aspect of data processing is understood as it entailed the collecting, storing, using and communicating of information.[496] Noting that in it lies the threat to right to privacy in two ways to wit first the compilation and distribution of personal information creates a direct threat to the individual's privacy and secondly, the acquisition and disclosure of false or misleading information may lead to an infringement of his identity.[497]

Indeed, the Court further urged for strict protection of privacy in online data processing through gadgets such as computers and mobile phones to conduct businesses, correspond, impart ideas, conduct research, explore their intimate life, seek medical advice and treatment, correspond in privileged circumstances, communicate with loved ones, express political and personal views, keeping records, arranging travel and conducting financial transactions.[498]

493 Kenya Human Rights Commission v Communications Authority of Kenya & 4 Others Constitutional Petition 86 of 2017

494 Ibid

495 Ibid

496 Ibid

497 Ibid

498 Ibid

The Court was alive to the power of the internet and its interconnectedness with the citizens' personal and professional since it has replaced the offline modes and means of operations which calls for more action on the part of state actors as the threat to privacy lurks within and without borders of states.[499] That obligation can be negative content requiring the state and its agents from violating right to privacy or positive content demanding that necessary measures be taken by state actors to protect the privacy of the individual[500] akin to precepts under Articles 20 and 21 of the Constitution of Kenya.[501]

The High Court in arriving at its decisions relied heavily on decisions from United States, Australia, South Africa, European Union, International Conventions and Treaties.[502] However, it is evident from the Court decision that save for the Constitutional provision and definitions from the Kenya Information and Communications Act there are no laws or regulations that it relied on to found its holdings on the right to privacy.[503] The High Court decisions clearly magnify lack of legislation on protection of right to privacy thus causing deficiency in our legal regime thereby limiting the full realisation of the constitutional right to privacy.[504]

4.5 Data from interviews:

The interviews conducted by way of questionnaires from 50 active social media users in different places in Kenya showed that many net users are apprehensive of protection of their privacy and data. They believe that both public and private actors have high chances of breaching their privacy

499 Ibid

500 Ibid

501 Constitution, 2010 Art.20-21

502 Kenya Human Rights Commission v Communications Authority of Kenya & 4 Others(2018)eKLR

503 Ibid

504 Ibid

in communication. They suggested more regulations on protection of privacy and that the same be made public so that the level of awareness is enhanced.

These views are in harmony with the findings from the secondary data and that the demands for more protection of privacy and data clearly show the urgency with which the law on protection of privacy should be implemented.

4.6 Conclusion

The Constitutional basis of right to privacy in Kenya has been highlighted in this Chapter starting with the analyses of this right in the 1963 Constitution and progressing to the 2010 Constitution. It is notable that the Constitution, 2010 has broadened the right to privacy to cover person, property, possessions, personal/family information or affairs and communication. Thus, the online connectivity and online interactions on social networking sites are covered. It also establishes that the slow growth on the legal regime about privacy has been contributed to by the development of the internet and technology in Kenya noting the government restrictions prior to 2002 general elections.

The jurisprudence on right to privacy in Kenya has been highlighted. Notably the Courts have decried the absence of enabling legislation hence the application of international law and best practices. Based on the enactment of Data Protection Act, 2019 it is believed that the Courts and all agencies charged with law enforcement will find easy time in tackling breach of privacy and data while at the same time proposing reforms to the Act for full realization of Article 31 of the Constitution.

CHAPTER FIVE

CONCLUSIONS AND RECOMMENDATIONS

5.1 Conclusion

This project was to establish whether the right to privacy under Article 31 of the Constitution, 2010 has not fully been realized because of absence of a specific legislation on protection of privacy.

Review of the Kenyan legal regime on right to privacy has clearly demonstrated various loopholes including absence of specific legislation to provide for regulation, enjoyment, limitation and enforcement of right to privacy. However, it is equally notable that since independence Kenya made some failed actions towards protecting the right to privacy but entrenching the right to privacy in the Constitution, 2010 was the most outstanding action which is memorable to date.[505] The enactment of Data Protection Act, 2019 is also a positive step towards protection of the right to privacy.

Indeed, privacy in the Constitution of Kenya has been classified as the most progressive in Africa noting that it is broader than a similar right in the Constitutions of both South Africa and Ghana. Further, the recognition of international conventions, principles and laws as part of laws of Kenya

505 Constitution of Kenya,2010 Art 31

clearly enhances the environment for possible enjoyment of right to privacy and will offer a good platform for enforcement of the Data Protection Act, 2019 in light of the provisions of GDPR.[506]

The right to privacy especially online has caught the attention of various international institutions and the United Nations has led the way by seeking to ensure that privacy enjoyed offline ought to be replicated online thus demanding for states to establish oversight institutions with administritaive, judicial and legislative powers to enable it consider instances of violations of privacy and award remedies or propose reforms in the existing law.[507]

The vision of the United Nations was manifested in European Union when it developed The European Data Protection Regulation (GDPR)[508] which has confirmed protection of data as a fundamental right and also imposed various obligations on various institutions charged with collection, processing, retention and sharing of private information. GDPR has limitless jurisdictional application in its attempts to protect the private data of the citizens from member states of European Union.

The increased access of social networks by Kenyans calls for urgent action to be taken towards regulating the right to privacy in social networking sites as envisaged in the obligations of Data controllers and processors. By March, 2019 the Communications Authority projected the increased usage of access to internet at 43,329,434 people compared to 200,000 people in 2000

506 Ibid Art 5 and 6

507 http://dag.un.org/bitstream/handle/11176/158167/A_RES_69_166-EN.pdf?sequence=3&isAllowed=y; Human Rights Council, The Right to Privacy in the Digital Age accessed on 10/10/2019

508 Directive 2016/679 to replace the 1995 Data Protection Directive (Directive 95/46/EC)

hence the internet growth of 21,564%. [509] Besides, there are emerging technological advancements which take place on a daily basis thus creating uncertainty of risks and threats.

The accessibility of the internet by phone and the affordable rates by the internet service providers and telecommunications companies, mobile to mobile access coupled by availability of computers and other internet enabled devices have enticed large population mainly the youths to enjoy the online life thus calling for urgent regulation to protect right to privacy and data while alleviating attendant risks and dangers.

The information accessed towards actualizing this project clearly demonstrates significant growth in online activities both locally and internationally which consequently poses risks and challenges in enforcement of right to privacy which calls for urgent regulation of these platforms to ensure full realization of right to privacy.

Chapter two has analysed the historical background of right to privacy and intertwined the same with modern technological developments. It has also assessed the place of right to privacy and its relationship to data protection with the conclusion that in Kenya these terms are synonymous while in other jurisdiction they have different scopes. The impact of the internet and technology on the right the privacy has been noted to the extent that the likely laws and regulations must be in sync with modern progress.

It is notable that traditional international law territories are being challenged by cyber space, cyber sovereignty and data autonomy hence the need to harmonize the local legislation on privacy with international laws on cyber space and best practices.

509 www.internetworldstats.com accessed on 10/10/2019

Chapter three has established the challenges of enforcement of privacy in Kenya until 2010 when Constitution, 2010 broadened the right to privacy to cover person property, possessions, personal information, affairs and communications thereby covering cyberspace and telecommunications channels and after several attempts to secure a comprehensive law to realize the gains made by promulgation of the Constitution, 2010 the Data Protection Act was enacted and operationalized on 25/11/2019 thereby bringing closer the actual realization of the rights under Article 31 of the Constitution.

Besides, the judicial struggle of enforcing the right to privacy has been demonstrated by various decisions. Notably the Courts have decried the absence of enabling legislation hence the application of international law and best practices. In as much as the Courts are guiding the enforcement of the right to privacy, it must be noted that there are numerous instances where victims of violation of right to privacy do not escalate the same to Courts either because of ignorance or due to fear of further exposure. Thus, based on the Data Protection Act, 2019 the Judiciary, Office of the Data Protection Commissioner and other agencies will find it easy in to fully realize the aspirations of Article 31 of the Constitution, 2010.

Chapter four has ventilated inadequacies in the legal regime on right to privacy in Kenya noting that the absence of specific legislation was an impediment to full realization of the broad constitutional underpinning of the right to privacy under Article 31. It is concluded that the available legislation had failed to address the modern threats to privacy especially online and that Data Protection Act, 2019 has arrived at the right time. The desire to protect privacy is evidenced by various failed attempts by legislature in Kenya towards enactment of Data Protection Act, 2019.

All the Bills highlighted in this Chapter note the issues of technological developments and modern threats and risks online and it is out of the said Bills that the Data Protection Act, seemed to have borrowed immensely from regional and international instruments to reflect its robustness. All expectations on realization of aspirations under Article 31 of the Constitution now remain in the process of implementation and enforcement of Data Protection Act, 2019.

To further show inadequacies in Kenyan privacy laws and progress made by enactment of Data Protection Act, 2019 the Chapter discussed data protection laws in South Africa and Ghana which have managed to implement their various legislation on data protection. Both countries having specific legislation and institutions of enforcement of right to privacy while their laws also reflect the principles contained the African Union Convention on Cyber Security and Personal Data Protection and the General Data Protection Regulation (GDPR) which recognizes right to privacy as fundamental right, imposing obligations on data processors and controllers while guaranteeing rights of subject data. Indeed, Data Protection Act, 2019 is equally reflective of all the principles of international practices in protection of privacy.

5.2 Recommendations

Right to privacy is a fundamental right, albeit not absolute, there is need to educate and/or sensitize members of the public of this right and risks, threats and likely violations of this right in technological environment and online platforms.

1. Reconciling the Data Protection legislation with other laws Kenya has statutes dating as far back as pre-independence. Some of these statues contain provisions that override this proposed bill, thereby threatening the good intentions of this framework. Such laws include: Preservation of Public Security Act,[510] Official Secrets Act,[511] National Intelligence Service Act, 2012 and The Prevention of Terrorism Act[512] just to name but a few. These laws have provisions authorizing the government to collect, process, and share data without consent in circumstances that are not well defined and therefore subject to misuse. There is need for realization of strong protections contained in this legislation hence recommendation that a package of amendments be offered to revise the provisions in current legislation.**[513]**

2. The Data Protection Act, 2019 has explicitly addressed the protection of data stored in the "cloud" (synchronized storage centres for digital data) and online generally by imposing obligations on data controllers and processors. [514] The issues of data autonomy and sovereignty to tackle external threats has been captured. It is recommended that the Data Protection Act, 2019 be implemented expeditiously by establishing relevant institutions and registering data controllers/processors and fully enforcing rights of data subjects.

3. The enforcement of right to privacy will be a reality if Data Protection Commission, a specialized agency, is established expeditiously and fully operationalized by being equipped by adequate resources and skilled personnel. It should have been empowered to hear and

510 Chapter 57 of Laws of Kenya

511 Chapter 187 of Laws of Kenya

512 No 30 of 2012 Laws of Kenya

513 Submission of Comments on the Kenya Privacy and Data Protection Bill, 2018 available at https://ca.go.ke/wp-content/uploads/2018/11/Mozilla-Submission-of-Comments-Kenya-Privacy-and-Data-Protection-Bill-2018.pdf accessed on 12/10/2019

514 State of Privacy Kenya, available at https://privacyinternational.org/state-privacy/1005/state-privacy-kenya accessed on 12/10/2019

determine disputes and complaints of violations and breach of right to privacy and abuse or misuse of data.

4. The proposals of the Senate in their 2018 Bill should be reviewed and identified so that they may be considered within the existing framework especially in light of the discretion bestowed on the Data Commissioner to develop rules and regulations for efficient implementation of the Act and enforcement of rights envisaged therein.

BIBLIOGRAPHY

BOOKS AND ARTICLES

Baezner M and Robin P, Trend Analysis: Cyber Sovereignty and Data Sovereignty, Center for Security Studies (CSS), Zurich – Switzerland (2018).

BalGanesh S and Mitra N, 'Cryptography, Privacy and National Security Concerns', Law Relating to Computers, Internet & E-commerce' (Universal Law Publishing Co Pvt Ltd 2013).

Banisar D, Freedom of Information and Access to Government Records Around the World (Privacy International, 2002).

Cavoukian A, Informational self-determination- the power of an individual to reveal personal data. As defined by Go Beyond Security- Build in Privacy, at <http:/www.eff.org/pub/Privacy

Cavoukian A, 'Privacy by Design' (Identity in the Information Society 2010)

Cohen R, Internet History, (International Journal of Technoethics (2011).

Communications Authority, "Quarterly Sector Statistics Report (2010)

Cooley T.M, A Treatise on the Law of Torts (Callaghan and Company 1888).

Crisci C.L, 'All the world is not a stage: Finding a right to privacy in existing and proposed legislation (N.Y.U Journal of Legislation and Public Policy, 2002).

Digital Watch Observatory (2017)

Devlin P, The Enforcement of Morals (Oxford: University Press, 1959)

DeVries W, 'Protecting Privacy in the Digital Age' (Berkeley Technology Journal (2003)..

Feldman D, Human Dignity as a Legal Value (1999).

Francisca Mweu, "Overview of the Internet in Kenya, (International Telecommunication Union, 2000)

Froomkin M, 'The Death of Privacy, Stanford Law Review (2000).

Hart H.L.A, Essays in Jurisprudence and Philosophy (1983).

Harvard Law Review Association, 'The Right to Privacy' Harvard Law Review(1898).

Jaishankar k (Ed) Book Review of Hate Crimes in Cyberspace, Centre for Cyber Victim Counselling (CCVC), International Journal of Cyber Criminology, (2014).

Judith T, 'The Right to Privacy' (Philosophy and Public Affairs, 1975).

Juma V, "Mobile Internet on Course to Becoming Top Earner for Firms, (Business Daily, 2010).

Knight S, 'All-Seeing Google Street View Provokes Privacy Fears', The Times (2007).

Kokott J and Sobotta C, The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR, *International Data Privacy Law*, (2013).

Leiner B.M et al, A Brief History of the Internet, Internet Society, (1997)

Lillich B.R, The Human Rights of Aliens in Contemporary International Law, (Manchester University Press 1984).

Logeais E and Schroeder J, The French Right of Image: An Amiguous Concept Protecting the Human Persona, (LOY. L.A. ENT. L. REV. (1998).

Lukács A, 'What is Privacy? The History and Definition of Privacy,' University of Szeged, Paris 1(2016) available at http://publicatio.bibl.u-szeged.hu/10794/7/3188699.pdf

Matyáš v, et al., The Future of Identity in the Information Society, (Springer Brno Czech Republic, 2008).

Moore R and Murray M, 'Right of Privacy', Media Law and Ethics (Routledge 2012).

Mureithi M, The internet Journey for Kenya: The Interplay of Disruptive Innovation and Entrepreneurship in Fueling growth in B. Ndemo, T.Weiss, (Eds), Digital Kenya: An enterpreneural revolution in the making (Palgrave Studies of Entrepreneurship in Africa. (Palgrave Macmillan (2017).

Mutemi M, Taming The Internet: The good, the bad and the ugly parts of the Computer Misuse and Cybercrimes Act (2018).

Noorani A, 'The Right to Privacy' (Economic and Political Weekly 2005)2.

Prosser W, 'Privacy' (48 California Law Review 1960).

Reed C, 'Electronic Privacy and Access to Information', Computer Law (Oxford University 2011).

Robertson A. H, Privacy and Human Rights (1st Edition, Manchester University Press 1973).

Rolph D, 'Politics, Privacy and the Public Interest: A Case Study from Australia (2018).

Sedley S, 'Towards a Right to Privacy'(London Review of Books2006).

Simmons J, Justification and Legitimacy, (109 Ethics 1999).

Smolin D, 'The Jurisprudence of Privacy in Splintered Supreme Court (Marquett Law Review 1992).

Solove D, 'A Brief History of Information Privacy Law' GW Law Faculty Publications (2006).

Solove D. and Paul S. M., ALI Data Privacy: Overview and Black Letter Text (2019).

Vakul S, 'Offence-Breach of Confidentiality and Privacy', Information Technology Law and Practice, Law & Emerging Technology Cyber Law & -Commerce (Universal Law Publishing Co Pvt Ltd 2007).

Warren S and Brandeis D, 'Right to Privacy' (Harvard Law Review(1890).

Westin A, 'Privacy and Freedom', Privacy and Freedom (Bodley Head 1970).

Whittle S and Cooper G, 'Privacy, Probity and Public Interest' (Reuters Institute for the Study of Journalism University of Oxford, 2008.

William B, Commentaries on the Laws of England, (Clarendon Press at Oxford 1769).

The Tallinn Manual on the International Law Applicable to Cyber Warfare and the Tallinn Manual 2.0

WEBSITES

http://www.internetworldstats.com

http://www.parliament.go.ke/sites/default/files/2017-05/Data_Protection_Bill_2018.pdf

https://www.acts.co.za/constitution-of-the-republic-of-south-africa-act-1996/index.html

http://www.justice.gov.za/inforeg/docs/InfoRegSA-POPIA-act2013-004.pdf

https://www.michalsons.com/blog/data-privacy-in-south-africa/150

http://www.itu.int/ITUD/projects/ITU_EC_ACP/hipssa/Activities/SA/docs/SALegislation/South %20Africa/ElecComm.PDF

https://www.privacy-europe.com/european-privacy-framework.html

http://dag.un.org/bitstream/handle/11176/158167/A_RES_69_166-EN.pdf?sequence=3&isAllowed=y;

http://kenyalaw.org

https://www.theelephant.info/features/2018/05/24/taming-the-internet-the-good-the-bad-and-the-ugly-parts-of-the-computer-misuse-and-cybercrimes-act-2018/

Human Rights Council, The Right to Privacy in the Digital Age available at http://dag.un.org/bitstream/handle/11176/158167/A_RES_69_166-EN.pdf?sequence=3&isAllowed=y;

www.internetworldstats.com

http://undocs.org

http://www.un.org

https://www.cfr.org/report/reforming-us-approach-data-protection

http:/www.eff.org/pub/Privacy

https://www.oecd.org

http://publicatio.bibl.u-szeged.hu/10794/7/3188699.pdf

http://www1.worldbank.org/publicsector/learningprogram/Judicial/AccessInfoLaw%20Survey.rt

https://digitalcommons.lmu.edu/elr/vol18/iss3/5

https://hostingfacts.com/internet-facts-stats/

https://www.businessdailyafrica.com

https://www.un.org/en/universal-declaration-human-rights/

http://technology.timesonline.co.uk/tol/news/tech_and_web/article1870995.ece

SAMPLE QUESTIONNAIRE

1. Do you have any social media account?

……
……

   a. If yes, do you fear that your data or information may be tempered with?

……
…….....

   b. If yes, do you think the suspects are from public or private entities or just individuals?

……
…….……

2. Do you believe that your right to privacy is protected by laws online or offline?

   a. Online……
   ……..

   b. Offline……
   ……

3. Make suggestions on how you wish your data to be protected

   ……
   ……

   ……
   ……

   ……
   …….